SEGURIDAD EN SERVIDORES LINUX NOTA 4



$8,80 EN TODO EL PAÍS

#26

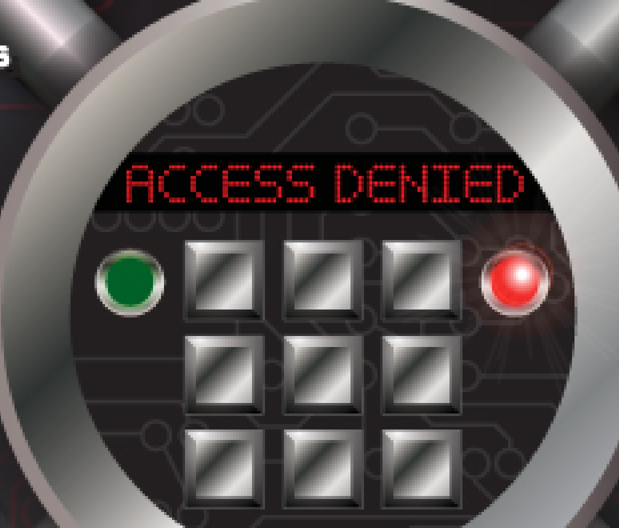
NEX IT SPECIALIST #26



SECCIÓN ESPECIAL CISCO SYSTEMS

Gusanos y Virus
Seguridad integrada contra epidemias

Network Services
Seguridad



Google
como herramienta de ataque

ESPECIAL SEGURIDAD

DDoS
Distributed Denial of Service

Detección de Malware
Conozca un laboratorio por dentro

Protección
Anti-spyware

WWW.NEXWEB.COM.AR
ISSN 1668-5423
Dist. Cap.: Vaccaro Sanchez y Cía. S.C. - Interior: DGP
Correo Argentino FRANQUEO A PAGAR Cta. 10185

INNOVADORES IT
APRENDA CON LOS MEJORES
"Liberando las Redes de los Ataques DDoS"
Edmund Lam, Cisco's Service Provider Systems Engineering Group

- ESPECIAL SEGURIDAD -



DIRECTOR
- Dr. Carlos Osvaldo Rodriguez

PROPIETARIOS
- Editorial Poulbert S.R.L.

COORDINADOR EDITORIAL
- Carlos Rodríguez Bontempi

RESPONSABLE DE CONTENIDOS
- Dr. Carlos Osvaldo Rodríguez

DIRECTOR COMERCIAL
- Ulises Román Mauro
umauro@nexweb.com.ar

SENIOR SECURITY EDITOR
- Carlos Vaughn O'Connor

EDITOR TÉCNICO
- Alejandro Cynowicz
redaccion@nexweb.com.ar

DISEÑO Y COMUNICACIÓN VISUAL
- DCV Esteban Báez
- Carlos Rodríguez Bontempi

DISTRIBUCIÓN
distribucion@nexweb.com.ar

SUSCRIPCIONES
- Maximiliano Sala
- Andrés Vázquez
- Martín Guaglianone
suscripciones@nexweb.com.ar

PREIMPRESIÓN E IMPRESIÓN
IPESA Magallanes 1315. Cap. Fed.
Tel 4303-2305/10

DISTRIBUCIÓN
Distribución en Capital Federal y Gran Buenos Aires: Vaccaro, Sánchez y Cia. S. C. Moreno 794, Piso 9. C1091AAP- Capital Federal Argentina.
Distribuidora en Interior: DGP Distribuidora General de Publicaciones S.A. Alvarado 2118/56 1290 Capital Federal - Argentina
NEX IT Revista de Networking y Programación
Registro de la propiedad Intelectual en trámite leg número 3038 ISSN 1668-5423
Dirección: Av. Corrientes 531 P 1
C1043AAF - Capital Federal
Tel: +54 (11) 5031-2287

Si desea escribir para nosotros, enviar un e-mail a:
articulos@nexweb.com.ar



Nota del Editor

Mantener nuestra empresa protegida de las muchas amenazas existentes parecería ser una batalla en la que tenemos pocas chances de ganar. Pero, es posible ganarla. Para ello debemos estar muy preparados. Debemos anticiparnos con estrategias, herramientas y técnicas correctas.

Hay muchos flancos en la batalla para asegurar nuestras redes. Por ejemplo, tan sólo la seguridad relacionada con el correo electrónico nos trae un abanico de temas en los que debemos ser expertos. Debemos conocer como combatir el spam, detener los virus hasta detener los ataques DDoS (Distributed Denial of Service). Y las soluciones por supuesto, no son las mismas si somos un usuario final, el administrador del servidor de correo en una PYME o a cargo de la infraestructura de red de un ISP (Internet Service Provider).

Nuevamente dedicamos un ejemplar de NEX IT Specialist a seguridad informática. La razón es muy simple y está reflejada en los dos primeros párrafos de esta Editorial. La seguridad informática sigue siendo de mucho interés y para quien trabaja en IT, networking o como programador (desarrollador) un rubro en el que debe capacitarse en forma constante y estar al día. Más aún, siendo ésta una disciplina donde la salida laboral es amplia, con buenos sueldos y las oportunidades abundan.

En los diferentes ejemplares de NEX hemos barrido desde temáticas básicas, dando los fundamentos hasta la descripción de productos con artículos realizados por los expertos de los vendors. Cada vez que debemos programar NEX nos resulta a veces difícil decidir que tipo de artículos incluir, y por eso tratamos de hacer un balance entre los productos y las tecnologías bases sobre las que éstos están construidos.

Creemos que ambos tipos de artículos deben estar presentes ya que es fundamental para el IT PRO/networker/desarrollador/CIO (es decir nuestros lectores) conocer las tecnologías como así también la oferta de los vendors y las tendencias del mercado si desea estar en la vanguardia en su expertise (preparación).

Quien es lector de NEX y posee toda nuestra colección, encontrará que casi todos los aspectos de la seguridad informática han sido cubiertos. Por ejemplo, quienes estudien la certificación más prestigiosa de seguridad informática, CISSP del ISC2 (www.isc2.org), hallarán prácticamente todos los dominios del CBK (Common Base Knowledge) descriptos y discutidos, descripción de la certificación, de su examen, los mejores libros disponibles. Aún, preguntas ejemplo para conocer qué es CISSP más profundamente.

Tal como nos definimos cuando comenzamos a planificar los objetivos y perfil de NEX, NEX es un libro en cuotas. A ésto le agregaría que a diferencia de un libro, NEX nos permite una actualización continua.

Se que disfrutarán de este ejemplar y como siempre, no dejen de contactarnos a ***redaccion@nexweb.com.ar***


☐ SOPORTA UNA PLATAFORMA DE GRAN ESCALABILIDAD
☐ GENERA CRECIMIENTO Y VALOR AGREGADO PARA LOS CLIENTES
☐ AUMENTA LA CAPACIDAD DE USUARIOS
☐ ACELERA Y SIMPLIFICA EL SERVICIO
☐ ES LINUX
☐ O WINDOWS SERVER







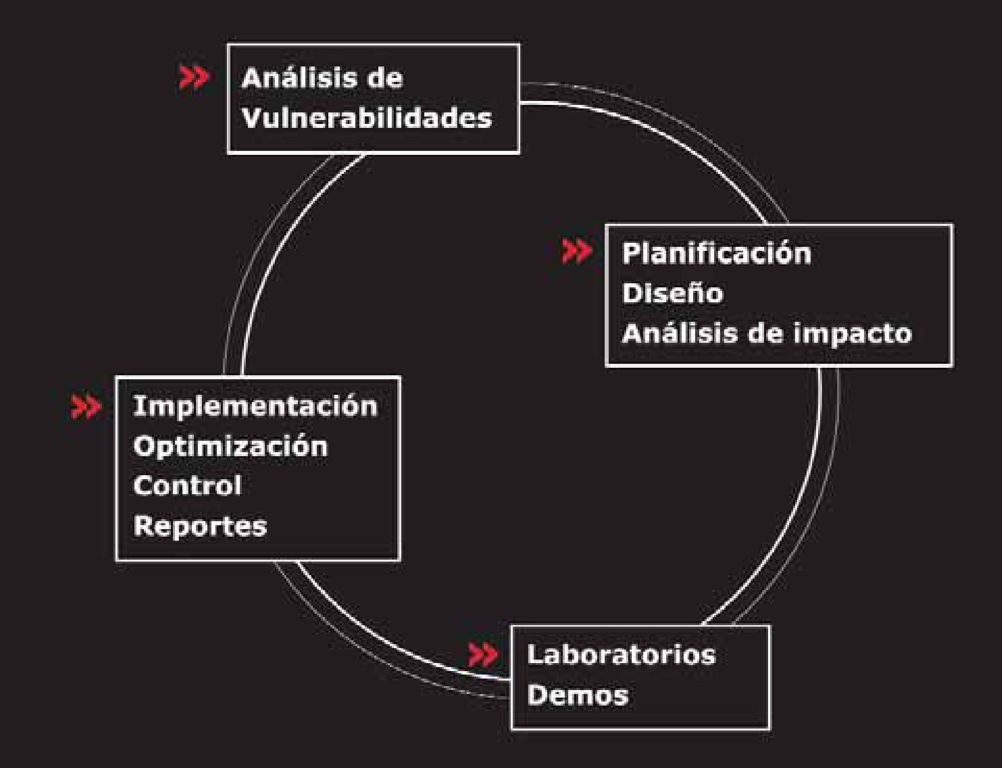
RED PUEDEN DESESTABILIZAR TODA SU EMPRESA.

SOFTNET LOGICALIS PROVEE LAS SOLUCIONES PARA PROTEGERLA,

minimizando los riesgos,

combinando Seguridad y Disponibilidad al mejor costo

y ofreciendo su expertise en:



- 60 técnicos altamente entrenados
- Más de 20 años de experiencia
- Primeros en implementar soluciones avanzadas de Seguridad (ASA - MARS)
- Soluciones integrales de Seguridad end-to-end
- Servicios gestionados de Seguridad (Softnet Security IDS)

THE LATIN AMERICA **NETWORKING** LEADER COMPANY

+54 (11) 4344-0333

info@la.logicalis.com

www.la.logicalis.com

SUMARIO

34

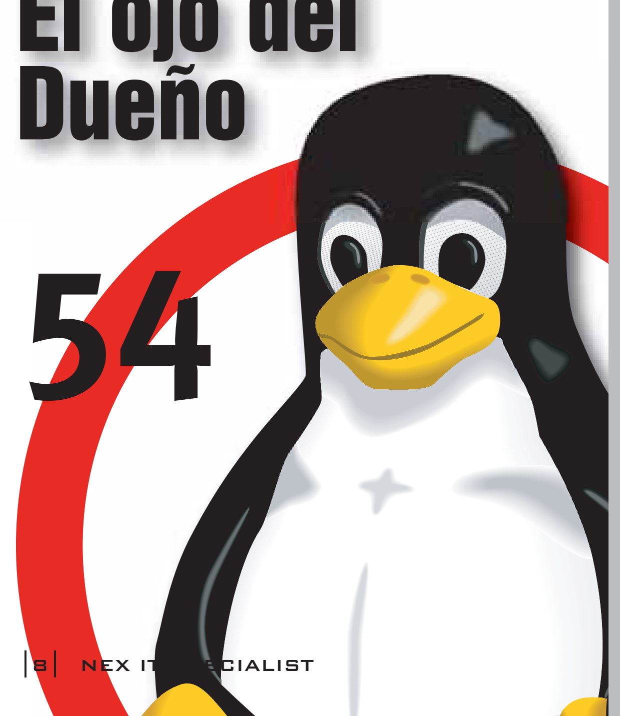
Google como herramienta de ataque

"Las fuentes de información públicas, como los buscadores, permiten a quienes lo deseen, acceder al menos al 80% de la información de nuestras redes, sin la necesidad de exponer su identidad"



Seguridad en Linux Nota 4. El ojo del Dueño

54



12



Arquitectura de red orientada a servicios

- 03 Nota del Editor
- 09 Eventos
- 11 Especial Cisco Systems
- 12 Arquitectura de Red Orientada a Servicios
- 18 Liberando las Redes de los Ataques DDoS
- 24 Gusanos y Virus
- 26 Ataque a los Datos en Argentina
- 30 Soluciones de Seguridad en Redes
- 34 Google como Herramienta de Ataque
- 42 Detección de Malware
- 44 Cómo estamos con eso de la Seguridad
- 46 Desafíos y Soluciones
- 50 Protección Anti-spyware
- 52 No es bueno que el hombre esté solo
- 56 TippingPoint
- 58 Seguridad en Linux Nota 4
- 64 Imposible no conocer Foundstone
- 66 Information Systems Security Assessment
- 72 Modelado y Diseño
- 78 Service Oriented Architecture
- 82 Breves / Humor

IMAGEN DE TAPA: Esteban Báez (c) - 2006

Gira Internacional de INETA Latam Cono Sur 2006

INETA Latam, en conjunto con los grupos de usuarios de tecnologías .Net de Latinoamérica y MSDN, organizó un nuevo encuentro Latinoamericano.

INETA - International .NET Association, es una organización independiente y sin fines de lucro, dirigida por una junta de líderes de grupos de usuarios elegidos por sus pares y respaldados por **Microsoft Corporation** y otros patrocinantes. Su misión es proporcionar asistencia, recursos y soporte a los grupos de usuarios de todo el mundo interesados en la plataforma .NET de Microsoft. Alberga a todos los miembros de la comunidad de usuarios .NET, desde desarrolladores y arquitectos hasta gerentes de proyecto y profesionales de IT.

Desde hace tres años **INETA Latam**, su filial Latinoamericana, organiza una gira anual por varios países de la región. El pasado 2 de Junio, en las instalaciones de la **Universidad Católica Argentina**, tuvo lugar el encuentro correspondiente a Buenos Aires.

En esta oportunidad expertos regionales e internacionales presentaron las últimas novedades en **"seguridad en el desarrollo de Software"**.

La apertura del evento estuvo a cargo de Nilda Díaz, Gerente de Proyectos **INETA-LATAM** y miembro responsable del Comité de Contenido Web de **INETA LATAM**. Nilda habló sobre la misión de Ineta y de los grupos de usuarios. En las presentaciones técnicas disertaron gurúes de la talla de **Pierre Jacomet, Wiernik Adolfo, Seara Daniel y Serrano Eugenio**. **Pierre Jacomet, Coordinador de Programa Windows - Grupo de virtualización de sistemas de Microsoft Corp**, habló de "Seguridad basada en roles para aplicaciones corriendo sobre Windows. Lo nuevo en Windows Vista". Mas tarde, **Serrano Eugenio, MVP ASP.NET**, nos contó como "Desarrollar Aplicaciones ASP.Net 2.0 Seguras" A continuación, **Wiernik Adolfo, Microsoft Regional Director de Costa Rica**, profundizó sobre "Interacción Segura con SQL Server 2005"

La última presentación técnica estuvo a cargo de **Seara Daniel, MVP Visual Basic.NET**, quien habló de "Seguridad para desarrolladores en SQL Server 2005".

El evento fue posible gracias a la colaboración de **MSDN, Programa Académico Microsoft** y los grupos de usuarios **Desarrollador@s y msJovenes** miembros de **INETA** en Argentina. También ayudaron el **Grupo de Usuarios Microsoft (MUG)**, y numerosos auspiciantes, entre ellos **Nex IT**, que regaló revistas a los asistentes y **CentralTECH** que entregó obsequios para sortear entre el publico. Eventos como este fortalecen los lazos entre los miembros de la comunidad y construye un espacio de comunicación e intercambio de información.

Para descargar las presentaciones de este evento visite los siguientes vínculos:

http://www.mugcordoba.net.ar/Default.aspx?Item=Eventos.htm

http://www.desarrolladoras.org.ar/novedades.htm



AVAYA

AVAYA CONNECT 2006 World Cup Edition

Más de 1000 personas participaron en el principal evento de comunicaciones Inteligentes del año

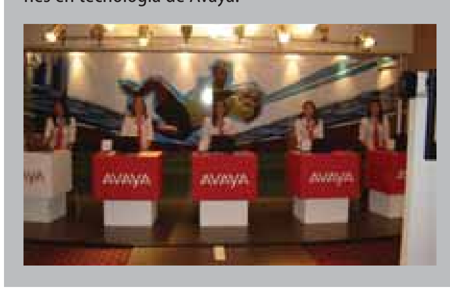
El martes 23 de Mayo se llevó a cabo el AVAYA CONNECT 2006 World Cup Edition, el mayor evento que organiza año a año Avaya Inc., uno de los principales proveedores mundiales de aplicaciones, sistemas y servicios de comunicaciones para empresas.

Durante la jornada se hicieron presentes más de 1000 ejecutivos de la industria IT, incluyendo clientes, prospectos calificados y BusinessPartners de la región Cono Sur, que pudieron conocer en detalle la tecnología que Avaya implementará en la Copa Mundial FIFA(tm) 2006 además de las nuevas soluciones de Avaya para empresas medianas.

A su vez, el marco del lanzamiento mundial, especialistas reconocidos a nivel internacional y regional presentaron nuevas versiones de soluciones de comunicaciones de Telefonía IP, Contact Centers y Movilidad para empresas medianas.

Por su parte, clientes de Avaya entre los que se encontraron Swiss Medical, La Anónima, Arvato, DHL, entre otros, junto con BusinessPartners, compartieron sus experiencias, desde el origen del desafío, hasta los beneficios que han obtenido mediante la implementación de soluciones Avaya.

Como todos los años, AVAYA CONNECT 2006 World Cup Edition, fue una experiencia 100% interactiva, incluyendo demostraciones en vivo de las innovaciones en tecnología de Avaya.



CALENDARIO DE EVENTOS IT EN ARGENTINA PARA EL 2006

Fecha		Informes
	JUNIO	
22	**1er Jornada Nacional de Calidad en Software** - Sheraton Libertador.	www.worktec.com.ar - info@worktec.com.ar
	AGOSTO	
-	**Seguridad en Redes Wireless** - Buenos Aires Sheraton Hotel.	www.worktec.com.ar - info@worktec.com.ar
	SEPTIEMBRE	
19 y 20	**Consecri-Consetic 2006** - Sheraton Libertador.	www.worktec.com.ar - info@worktec.com.ar
-	**Soluciones de Seguridad Open Source** - Buenos Aires Sheraton Hotel	http://www.cybsec.com/capacitacion
	OCTUBRE	
3 al 6	**EXPO COMM** - La Rural, Predio Ferial de Buenos Aires.	www.expocomm.com.ar
6 y 7	**2do Congreso Nacional de Estudiantes de Sistemas y Tecnología de la Información.** - Lugar a confirmar.	www.worktec.com.ar - info@worktec.com.ar
-	**Business Continuity Planning** - Buenos Aires Sheraton Hotel	http://www.cybsec.com/capacitacion
	NOVIEMBRE	
2	**Jornadas Trabajo IT 2** - Sheraton Libertador.	www.worktec.com.ar - info@worktec.com.ar
2 al 5	**AES - Argentina Electronic Show** - La Rural, Predio Ferial de Buenos Aires.	www.aeshow.com.ar/es_services_contact_us

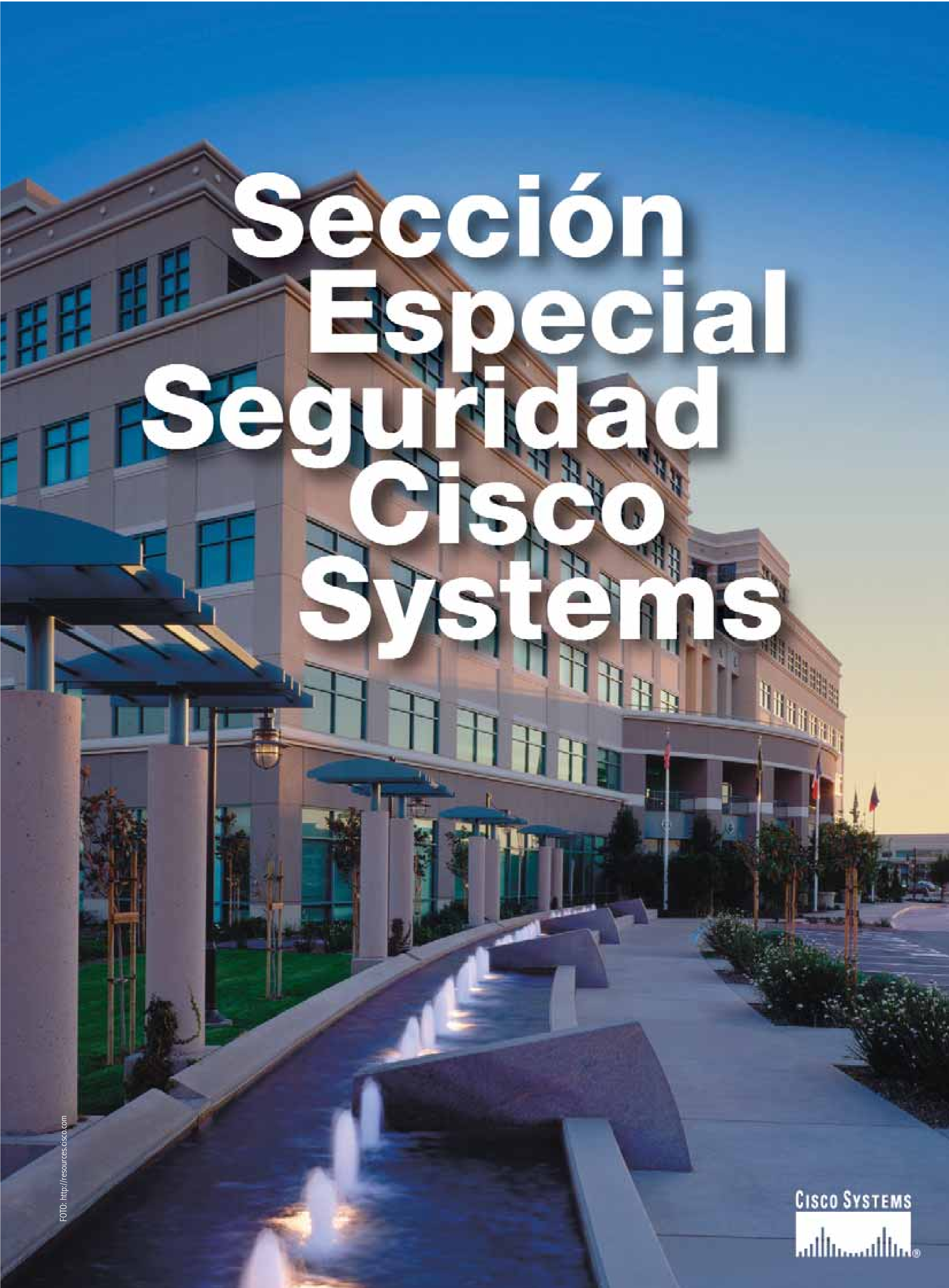
Si desea ver su evento IT publicado en esta sección, por favor háganos llegar la información respectiva a: eventos@nexweb.com.ar

Check Point Security Tour 2006

El 16 de Mayo se llevó a cabo el Check Point Security Tour 2006. Los temas que se abordaron durante el transcurso del mismo, se refirieron principalmente a la seguridad en: la conectividad de aplicaciones en dispositivos móviles, la expansión de redes remotas, la accesibilidad segura a redes, el aprovechamiento de VoIP, entre otros.

Tuvo una asistencia de más de 300 expertos, y contó con la participación de Websense, Nokia, Aladdin, radware y Crossbeam Systems.

Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.


Sección
Especial
Seguridad
Cisco
Systems
FOTO: http://resources.cisco.com
CISCO SYSTEMS

Arquitectura de red orientada a servicios

Por **Janet Kreiling**

La implementación de la seguridad como otros procesos de negocio de las empresas será más sencillo y con menores costos si pensamos los procesos como sentados sobre una arquitectura muy amplia: una arquitectura de arquitecturas.

Probablemente al menos uno de sus objetivos de negocios más inmediatos está en esta lista:

• Activar toda la cadena de abastecimiento antes de que el stock sea inexistente.
• Mejorar la seguridad o movilidad.
• Permitirles a ubicaciones en cualquier parte del mundo, trabajar fluidamente con las sedes principales y entre sí.
• Hacer que sus sucursales sean eficientes al ofrecer soporte a clientes o empleados remotos.
• Ofrecer entrenamiento eficientemente.
• Asegurar la rápida recuperación de los datos y operaciones luego de una interrupción
• Consolidar aplicaciones, operaciones de datos y almacenamiento lejos de silos verticales.
• Simplificar las operaciones IT; ahorrar capital y gastos operativos.

Lograr cada una de las metas, y cientos más será más fácil y menos costoso si Ud. aprovecha a máximo su red y también vuelve a pensar cuál es su visión sobre ésta.

Desde el data center corporativo hasta una oficina al otro lado del mundo, su red puede mejorar la manera en que le sirve a sus clientes; la manera en que crea e implementa nuevos servicios o productos; la forma en que potencia a los empleados; y el valor que obtiene de cualquier tipo de datos, sus procesos de producción, administración de inventarios y cadena de abastecimiento, sistemas financieros, y toda otra actividad en la que su empresa esté involucrada.

¿Irrealizable? En realidad, no. Pero primero, debe adoptar una nueva perspectiva en su red. Piense en todos sus procesos corriendo sobre una sola y amplia arquitectura (una arquitectura de arquitecturas, por así decirlo), por lo que hacen uso de los mismos recursos de red.

La Universidad Nacional de Singapur (NUS) comenzó a cambiar su perspectiva hace cinco años cuando decidió crear una red integrada y crear un portal online para estudiantes, profesores, y su personal para organizar sus actividades diarias. NUS quería crear un ambiente donde las oportunidades de aprendizaje rodearan a los alumnos las 24 horas del día, todos los días. También quiso flexibilidad para el futuro. Para que su portal de enseñanza en línea soportara una vasta cantidad de capacidades que pudieran ser expandidas a medida que se presentaran nuevas necesidades, NUS reemplazó la totalidad de su red

ACCESS DENIED

IMAGEN: Esteban Báez - 2006

Cisco Service-Oriented Network Architecture (SONA, Arquitectura de red Cisco orientada a servicios) delinea cómo las empresas pueden evolucionar sus redes para incrementar su eficiencia, recudir sus costos, y fortalecer la agilidad de los negocios. Conozca cómo la Universidad de Singapur ya lo implementó

por una infraestructura Cisco integrada. (Ver la pastilla adjunta)

SONA

Cisco ha desarrollado un framework llamado Service-Oriented Network Architecture (SONA) en el que toma forma el pensamiento adelantado que la Universidad Nacional de Singapur tiene sobre su red.

SONA marca cómo las empresas pueden evolucionar su infraestructura IT hacia una red inteligente de información que acelera las aplicaciones y maximiza los procesos y recursos de los negocios. El framework muestra cómo sistemas integrados a lo largo de una red totalmente convergida, permite flexibilidad, mientras la estandarización y virtualización de los recursos incrementa la eficiencia.

SONA tiene tres capas (ver figura 1 en la siguiente página). La capa de infraestructura de red es donde todos los recursos IT están interconectados usando una red segura y convergente. Esta capa abarca todos los lugares de la red: campus, sucursales, data centers, WAN/MAN, y trabajadores a distancia.

La capa interactiva de servicios le permite a las aplicaciones y procesos de negocios, recibir eficientemente los recursos, entregados a través de la infraestructura de red. Aquí residen servicios tales como seguridad, movilidad, almacenamiento, virtualización, y segmentación.

Lo que los define como servicios, en lugar de aplicaciones, es que los sistemas que los proveen dotan la red con varios componentes residentes en diferentes sistemas, y están disponibles a todos los usuarios, según Bridget Bisnette, Directora Global para Enterprise Solution Partners de Cisco. La seguridad, por ejemplo, requiere de firewalls, Network Admisión Control (NAC), detección y prevención de intrusiones y mucho más. Algunas funciones tienen base en el router; otras en los appliances de la red, pero todas son usadas colectivamente para brindar seguridad a los usuarios, aplicaciones y sistemas en toda la empresa.

"Los servicios de cómputo, voz, identidad, y almacenamiento son otros que comenzaron como aplicaciones pero evolucionaron hacia servicios que serían incluídos en la red, y ser administrados por ésta", dice Bisnette.

La capa de aplicaciones contiene las aplicaciones de negocios y de colaboración que impulsa la eficiencia de los servicios interactivos.

Estas aplicaciones están disponibles también para toda la empresa. Alguien en un call center en India puede acceder a los mismos datos del cliente en su computadora, de la misma copia de la aplicación CRM en el mismo data center, como si fuera un usuario en las oficinas centrales de la compañía en Europa o Norteamérica

Por debajo de la capa de aplicaciones y servicios, yace el concepto de virtualización, el cual va más allá del mero acceso hasta la disponibilidad. Para cualquier usuario, las aplicaciones y servicios de red están disponibles como si hubieran sido generados en los equipos de la sucursal más cercana, ya sea que el usuario se encuentre en las oficinas principales, o al otro lado del mundo. Dado que del 50 al 80 por ciento de los empleados no suelen estar en las oficinas principales, la virtualización debe intuitivamente mejorar la productividad, remarca Paul McNab, vicepresidente de marketing en el Integrated Networks Systems Engineering de Cisco.

La virtualización soporta la tendencia hacia la convergencia de voz y redes de datos, de servicios, y hasta de datos en sí mismos; los cuales deben ser protegidos a través de una red end-to-end integrada, con servicios de seguridad embebidos en ésta.

Al tener sólo una instalación de un CRM, enterprise resource planning (ERP), o de un programa de administración de almacenaje, ahorra todo el trabajo de replicar y actualizar los datos en copias en diferentes ubicaciones. Cuando los datos se actualizan a cada milisegundo, pueden ser usados por una aplicación tras otra, y la red puede asegurar que fluya de una aplicación hacia otras.

Es más, los datos y las aplicaciones pueden estar almacenados en cualquier servidor o dispositivo de almacenamiento que tenga capacidad disponible.

Lo que brinda la virtualización de los datos en cualquier empresa, dice McNab, es visibilidad a cualquiera dentro de ésta o aquellos que los necesiten más allá de la misma.

"Una cadena grande de distribución minorista, puede tener 5000 comercios y emplear a 5000 personas. La gente o aplicaciones en la tienda, en las oficinas principales, y toda la cadena de abastecimiento, donde sea que estén ubicados, les puede ser posible ver la información cuando una tienda en Los Gatos, California, vende algún producto", explica. "Esa comunicación, especialmente con todos los eslabones de la cadena de abastecimiento, se está transformando en algo crucial a medida que las compañías tienen que mantener un estricto seguimiento del inventario y un efectivo control de los gastos. La tarea por realizar, agrega, "ya no se trata de administrar el producto, sino los datos acerca del producto".

Haciendo Obsoletos los Silos

Las aplicaciones y el almacenamiento de datos necesitaban estar cerca de sus usuarios, por lo que la latencia de la red no se convertía en un problema. Simplemente no había el vasto volumen de aplicaciones que hay hoy.

Ahora, dice Grez Mayfield, Senior Manager en el grupo Enterprise Solutions Marketing de Cisco, es común que una empresa tenga cientos de aplicaciones y bases de datos en silos separados, con un montón de espacio libre en sus servidores, y hasta mil aplicaciones a la espera de ser instaladas y ejecutadas.

Cisco introdujo varios productos nuevos que optimizan la performance de las aplicaciones. Por ejemplo, la latencia puede ser curada por Application Velocity System (AVS) de Cisco, el cual minimiza tanto el número de transmisiones a lo largo de la WAN para usar una aplicación como su contenido. Wide Area Application Services, de Cisco, el cual almacena en cache información esta-

Una Arquitectura De Arquitecturas

Un solo talle, por supuesto, rara vez les calza a todos. El framework SONA de Cisco debe abarcar todos los lugares de la empresa. Por eso, Cisco ha creado "sub-arquitecturas" del modelo SONA para cada uno de esos lugares. La arquitectura de un campus, por ejemplo, está subdividida en áreas de acceso, distribución, y de áreas básicas. Guías de diseño para cada arquitectura aseguran que los sistemas instalados desempeñen las funciones necesarias en cada parte del total de la red y también que trabajen juntos en la totalidad de la misma. Tomemos por ejemplo las posibles variantes para las sucursales. "Hay varios tipos de sucursales. Un call center es una oficina sucursal," dice Jeanne Beliveau-Dunn, directora de marketing para Enterprise Routing y Switching en Cisco. "Pero la mayoría de las sucursales no tiene soporte IT residente, y sus redes son planificadas y enviadas desde las oficinas principales. Cisco ha tratado lograr la mayor integración posible de los servicios que puedan ser necesarios. La arquitectura de sucursales de SONA les muestra a los clientes el modo de implementar esas oficinas de modo de incluir, seguridad, confiabilidad, convergencia de servicios, telefonía IP, video, compartir archivos en áreas amplias, networking de contenidos, QoS, velocidad de aplicaciones, networking orientado a aplicaciones, o lo que sea que necesiten." Agrega Beliveau-Dunn, "Eso es de lo que se trata una gran parte del SONA: mostrar mejores prácticas para diseñar cualquier parte de una red."

Capa de Aplicación
PLM | CRM | ERP
HCM | Procurement | SCM
Capa de Colaboración
Mensajería Instantanea | Mensajería Unificada | Lugar de Encuentro
IPCC | Teléfono IP | Entrega de Video
Plataformas de Aplicaciones y Middleware

Capa de Servicios Interactivos
Entrega de Aplicaciones
Redes Orientadas a Aplicaciones
Services Virtualization
Servicios de Seguridad
Servicios Móviles
Servicios de almacenamiento
Servicios de Infraestructura
Servicios de Voz y Colaboración
Servicios de Cómputos
Servicios de Identidad
Servicios de Administración Adaptativos
Virtualización de la Estructura de Red
Administración de Infraestructura

Capa de infraestructura de red
Campus | Sucursal | Centro de Datos | Empresa | WAN/MAN | Trabajador a distancia
Servidor | Almacenamiento | Clientes

Arquitectura de red Cisco orientada a servicios

ble localmente, también minimiza el tráfico WAN, al igual que el Cisco Content Services Switch y Cisco Content Services Module, el cual equilibra las cargas de peticiones a lo largo de múltiples servidores de aplicaciones de acuerdo a las políticas que asegura que las peticiones vayan al servidor correcto.

Un inconveniente recurrente al automatizar los procesos del flujo de trabajo, ha sido la imposibilidad de las aplicaciones para compartir datos entre sí porque emplean muchos lenguajes y protocolos distintos.

Los productos de, Application-Oriented Networking (AON), de Cisco, se ocupan de quitar ese obstáculo del camino. Un router blade AON funciona como un traductor universal para varias aplicaciones empresariales, lo que le permite a los datos moverse de una a otra sin interrupciones. El módulo AON habla en muchos lenguajes y protocolos; puede leer mensajes para ver que contienen y dónde debería ir la información. AON puede también aplicar políticas y prioridades a los mensajes.

El Rol de los Partners

Los productos AON mencionados anteriormente, demuestran el rol de Cisco en la capa de aplicaciones de SONA: facilitar su uso. Pero las aplicaciones en sí mismas y su integración en los procesos del flujo de trabajo son tareas que les corresponden a partners Cisco, dice Bisnette. De hecho, SONA recae en partners de Cisco para lo siguiente:

- Entregar los productos Cisco asociados con SONA, proveer el servicio de soporte y la administración general de los sistemas IT, requerido para brindar una solución completa, desde aplicaciones de negocio separadas hasta el diseño del ciclo vital de la red e implementación.
- Consultoría y reingeniería de los negocios, mientras que las compañías preparan sus redes para SONA, y proveer servicios administrados. En el futuro, las redes de próxima generación implementadas por proveedores de servicio se interconectarán firmemente con las arquitecturas SONA de sus clientes, por lo que las aplicaciones y los servicios hosteados pasarán de forma transparente de una a otra.

Cómo comenzar

Evolucionar hacia una red integrada y más inteligente con SONA se realiza en fases:

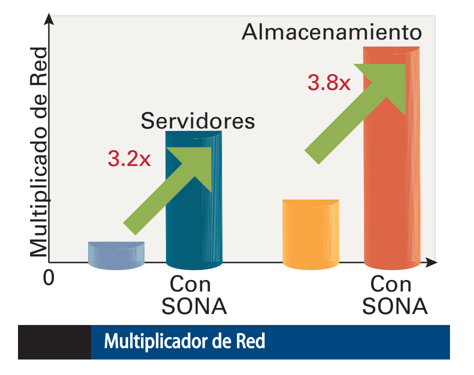


Figura 2 - La virtualización aumenta el porcentaje de bienes de red utilizados, a su vez mejorando la efectividad de lo gastado en tecnología. Este cuadro representa la experiencia del departamento IT de Cisco con la capacidad de los servidores: el uso de servidores fue 3,2 veces más efectivo con SONA que sin ésta; el uso de sistemas de almacenamiento fue 3,8 veces más efectivo.

Figura 1 - En la visión que Cisco tiene para SONA de uno a tres años en adelante, todos los recursos están interconectados en forma segura a través de una red convergente. En esta nueva visión de infraestructura de servicios, la red mejora las aplicaciones de forma significativa, con su habilidad de entregar servicios a usuarios finales de forma segura, optimizada, y adaptable.

Convergencia y estandarización de las redes a lo largo de toda la empresa. Las mejores empresas IT en su clase, están diseñando redes de voz/datos/video para manejar todas las comunicaciones de los negocios y estandarizando los componentes de las redes, escritorios, y servidores para optimizar y simplificar su infraestructura.

Consolidación de los recursos IT como servidores, cuyo uso es notoriamente bajo cuando se ubican en silos desparramados alrededor del mundo. Muchos son usados a sólo su 20% o 25% de su capacidad.

Virtualización de los recursos IT, como ser clustering de servidores, donde una aplicación dada o el almacenamiento de datos residen en unos pocos o un solo lugar central, en vez de docenas o cientos de ubicaciones. O networking virtual, el cual permite segmentar la red de forma segura para implementar sistemas de redes escalables, manejados y facturados separadamente, para soportar múltiples negocios. En ambos casos, la virtualización permite agrupar sistemas o asignaciones de tareas para maximizar los recursos y reducir costos y excesivos recursos administrativos.

Automatización, o implementar servicios basados en redes como ser seguridad e identificación a lo largo de la red para que todas las aplicaciones puedan y logren llamarlos. Las empresas también

invocan a la optimización de las aplicaciones en este nivel, agregando capacidades como AON, con sus servicios de traducción entre aplicaciones y administración inteligente de datos.
La clave de una migración efectiva, dice Mayfield, es pensar primero sobre el problema de los negocios, en lugar de la tecnología. ¿Cuál es el problema de su negocio que quiere resolver? ¿Cómo puede dirigirse mejor a este problema? Y luego, ¿Qué solución satisface las necedades inmediatas y crea una base para manejar futuras necesidades? Hay varias maneras de comenzar a migrar a una arquitectura SONA. agrega McNab, "la mayoría de la gente empieza con la red que tienen, en lugar de realizar una actualización de raíz. Podrían comenzar con un servicio o aplicación, tales como administración de archivos, verificación de identidad, o presencia de usuarios. La diferencia es que ahora buscarían cómo crear un servicio de identidad que trabaje en toda su empresa, en lugar de tan solo un departamento"

La Red Adaptable

Los productos de Cisco ya tienen un alto grado de interoperabilidad. Ud. puede crear una red integrada basada en SONA para todas las sub-arquitecturas de su empresa a partir de los productos disponibles. En los años venideros, dice McNab, Cisco trabajará para asegurar que todas las arquitecturas y productos individuales operen entre sí desde la perspectiva de las aplicaciones para proveer servicios de red. En síntesis, SONA es una red adaptable, una que puede brindar a una empresa la habilidad de reaccionar en tiempo real a nuevas oportunidades de negocios, cambios inesperados en los mercados, y demandas de los clientes. Eso es exactamente lo que Roland Yeo, administrador de redes en NUS, cree haber logrado. "Nuestra infraestructura Cisco satisfizo nuestras necesidades inmediatas, y ahora cinco años más tarde, podemos agregar servicios de seguridad, implementación de voz y aplicaciones de video, simplemente habilitando características QoS en la red."
La red basada en SONA ha cambiado la manera en que la NUS hace negocio, la forma en que educa a estudiantes y cómo los empleados interactúan unos con otros. Es realmente adaptable. Además, y la universidad también está ahorrándose U$S 1 millón tan sólo en costos de telefonía de voz. ■

La Universidad Nacional de Singapur: SONA en Práctica

La Universidad Nacional de Singapur (NUS) *tiene 13 facultades, 12 institutos de investigación de nivel universitario, 32000 estudiantes, y más de 3000 miembros e investigadores. NUS se propuso varias metas cuando decidió construir una red para soportar incontables aplicaciones multimedia incluyendo e-learning, transmisión de cátedras en vivo, telefonía IP, biblioteca digital y archivo de medios, administración del alumnado, admisiones a la universidad, registro de cursos, y GRID computing. Su red tenía que ser escalable, robusta, confiable, y alcanzar una alta performance para adaptarse dinámicamente a todas las demandas de tráfico asincrónico o sincrónico, ya sea en tiempo real o no.*
NUS recurrió a Cisco para obtener una red convergente e integrada y durante los cinco años que han pasado evolucionaron su infraestructura IT hacia una red inteligente y altamente disponible basada en el framework SONA de Cisco. La red distribuye servicios de seguridad, identidad, anexión inalámbrica, y storage por toda la organización. Les permite a los estudiantes y miembros de la facultad obtener cátedras vía Webcast, resultados de exámenes, tareas, materiales de la biblioteca, un sistema de mensajería, yo otros recursos a través del Integrated Virtual Learning Environment (IVLE). Con un servicio de conexión inalámbrica en toda la extensión del campus, les permite a los estudiantes acceder a materiales de sus cursos en cualquier momento y cualquier lugar usando notebooks. Con SONA, la experiencia de la conexión inalámbrica y cableada son iguales, comenzando por la seguridad. Los servicios de autenticación y autorización son consistentes entre ambas redes.
"Las aplicaciones como IVLE deben ser implementadas sin saber exactamente cual será la demanda o cuanta gente la usara simultáneamente," dice Roland Yeo, Administrador de la red en NUS. "La tienes que basar en una red escalable y asegurarse que los servicios de red que corren por debajo de ésta entregarán la aplicación cuando sea necesaria."
La red puede administrar políticas muy granulares para todos sus usuarios finales. Por ejemplo, un estudiante se puede loguear en el IVLE para rendir un examen en línea a través de una VPN segura pero mientras tanto, no puede acceder a ningún otro recurso dentro o fuera del campus. Las tarjetas de acceso con código, requerías para abrir todas las puertas en el campus, pueden rastrear los movimientos de los individuos en el campus en momentos de emergencias, lo que fue útil durante la crisis del SARS cuando la universidad necesitó saber quién pudo haber sido expuesto. La red también ha permitido nuevas aplicaciones críticas como Centralized Online Registration Systems (CORS) para selección y ubicación de módulos. "A medida que la universidad avanza hacia una educación de base más amplia, a los estudiantes se les requerirá que se enrolen en módulos a través de las facultades, y se debe establecer un sistema para facilitar una justa, equitativa y responsable selección de los módulos y al mismo tiempo, permitirles a los departamentos de enseñanza administrar sus recursos óptimamente.", explica Kwee-Nam Thio, administrador de los sistemas información académicos en NUS. CORS ha asignado exitosamente 1.200 módulos cada semestre a los más de 20.000 estudiantes registrándose en línea desde cualquier lado, dentro y fuera del campus.
"Nuestro reto más importante es balancear seguridad con apertura," dice Yeo. "La arquitectura Cisco SONA provee un framework para garantizar la seguridad, en lugar de intentos ad hoc para prevenir una amplia gama de amenazas a la seguridad." La flexibilidad se ha vuelto crucial, agrega, dado que la red está preparada para defenderse de amenazas, tales como ataques DoS (Denial of service), que eran desconocidos cuando la esta arquitectura fue instalada cinco años atrás.
Mientras que la universidad ha tomados pasos importantes hacia establecer un ambiente "e-enabled" (con acceso a las tecnologías) extensivo,



Tommy Hor, director del centro de computadoras en NUS, ve las siguientes áreas como importantes para las futuras capacidades IT del NUS: un entorno single-source, donde los reportes de la universidad provendrían de una herramienta central, creando una visión unificada a través de múltiples funciones departamentales; Integración de la voz, datos, y video, con más interfaces integradas para el audio, video, y llamadas Web con acceso simultaneo en tiempo real a bases de datos y aplicaciones que permiten la toma de decisiones de manera inteligente e informada; sistemas y dispositivos con tecnología inalámbrica para un acceso permanente a los recursos; portales personalizados para distribuir información en vez de diseminación de puros e-mails.
La arquitectura SONA de Cisco facilitará en gran medida en este viaje, dice Hor.


todo
bajo
control
poweredbycisco.
Mantenga siempre el control de su empresa.
La Red Auto Defensiva de Cisco ofrece un portafolio completo
de soluciones integradas de seguridad, optimizando su capacidad
para identificar, prevenir y responder a las constantes amenazas
que atentan contra su negocio. Con estas soluciones de seguridad,
Cisco y sus partners le ofrecen la habilidad
para reducir sus costos y dar continuidad a su negocio.
Transforme su red en una herramienta estratégica
y asegúrese una ventaja competitiva ingresando
a nuestro site para más información y promociones:
www.cisco.com/offer/segnexit
o comuníquese al 0810-444-CISCO (24726)
CISCO SYSTEMS
security. powered by
©2005 Cisco Systems, Inc. Todos los derechos reservados.

Liberando las Redes de los Ataques DDoS

Una solución integral les permite a los proveedores de servicios ofrecer nuevos servicios a aquellos clientes con especial interés en la seguridad.

Por **Edmund Lam**

FOTO: Purdue News Service photo/Dave Umberger



Que un ataque distribuido de negación de servicio (DDoS, Distribuited Denial of Service) haga caer una red corporativa, es más fácil de lo que Ud. cree. Los ataques DDoS son creados usualmente por botnets, redes de computadoras individuales (bots) comprometidas, que pueden ser dirigidas por un atacante para que lancen una oleada de varios tipos de paquetes hacia el objetivo. Un botnet relativamente pequeño puede contar con unas 1000 máquinas. Si estimamos una velocidad de subida de 128 Kbit/s por máquina, el botnet puede generar más de 100 Mbit/s de datos entrantes, más grande que muchas de las conexiones entre los proveedores de servicio y grandes empresas.

Peor aun, los ataques DDoS a redes relacionadas con negocios están creciendo a un ritmo furioso. El número de bots se está disparando, en gran parte a causa del incremento de las PCs hogareñas con conexiones a Internet permanentes las 24 hs., que frecuentemente están pobremente aseguradas y disponibles para los hackers. Muchos ataques son operaciones criminales serias, que amenazan con tener lugar durante importantes eventos corporativos.

Los ataques DDoS pueden saturar el ancho de banda disponible para las comunicaciones entrantes, salientes, e intranetwork; sobrepasan la capacidad de los routers, servidores, e incluso firewalls, volviéndolos, incapaces de atender al tráfico legítimo; previenen el acceso a aplicaciones o hosts específicos; atacan otros recursos de red como los soft switches, routers core, y servidores de Domain Name System (DNS), y causan daños colaterales a partes de la red que no fue atacada directamente. No es sorpresa, que un estudio del Grupo Gartner encontró que para la mayoría de las empresas, la seguridad de sus redes había escalado del décimo puesto de su lista de gastos en 2003, al primero en 2004.

Otro factor que influye en este problema creciente, es el hecho de que los ataques DDoS son difíciles de detectar, porque los paquetes ilegítimos no son fáciles de distinguir de los legítimos. El típico sistema de signature pattern matching, realizado por el sistema de detección de intrusos (IDS), no funciona. Algunas de las más populares técnicas para lidiar con los ataques DDoS, como el blackholing y el filtrador de routers, también se quedan cortos en términos de mitigarlos y asegurar la continuidad de los negocios. Estrategias como el sobre aprovisionamiento, no dan una adecuada protección contra ataques más grandes, y son soluciones de prevención de DDoS demasiado costosas de administrar.

"Cañerías Limpias"

La respuesta a los ataques DDoS es un sistema de protección que detecte ataques cuando comienzan, desvíe y "limpie" el flujo de tráfico contaminado, o tubería, y luego devuelva el tráfico legítimo a la red. Cisco ofrece ahora un sistema semejante llamado el Cisco DDoS Protection Solution que realiza todas estas tareas (ver figura 1). Puede ser implementado en proveedores de servicio para:

• Administrar la protección DDoS para sus clientes, en la última milla y dentro de la parte pública de su infraestructura.

• Proteger los servicios Web y aplicaciones de comercio electrónico en data centers de hosting administrados.

• Proteger los enlaces a los ISP (Internet Service Providers) de bajada, para evitar su saturación con tráfico DDoS.

Además, la solución le permite a los proveedores de servicio defender los elementos de su propia infraestructura de red crítica como routers y switches agregados, de límite y core, servidores DNS, y enlaces transoceánicos, casi en el mismo instante que el ataque es detectado.

Cisco DDoS Protection ofrece una solución abarcadora para brindar la capacidad de tener "cañerías limpias". Pero a los proveedores de servicios se les recomienda fuertemente que implementen medidas de seguridad conocidas como Cisco Network Foundation Protection (Ver Pastilla). Estas medidas fortalecen la seguridad de los datos, el control y administración de la infraestructura de un proveedor contra amenazas a su seguridad y permite un mejor posicionamiento para la entrega del servicio. Mientras, los elementos funcionales del Cisco DDoS Protection Solution —detección y mitigación (incluye distracción, limpieza, e inyección)— trabajan en conjunto para proteger a los proveedores de servicio y sus redes para clientes de los ataques DDoS.

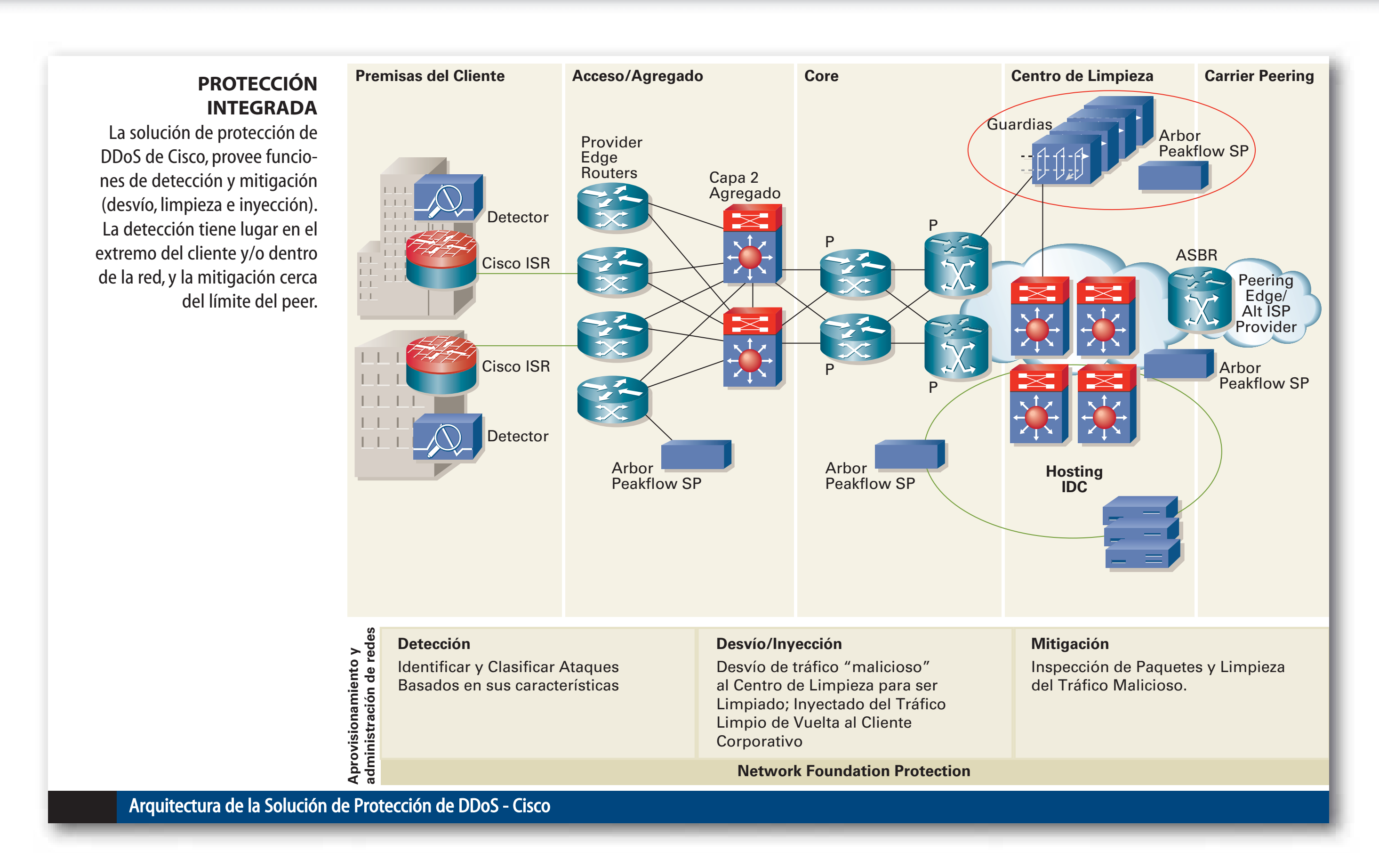
Detección

Históricamente, la detección de DDoS ha sido complicada, porque los paquetes ilegítimos tienen el mismo contenido y encabezado que los legítimos. Más aun muchos ataques usan direcciones de origen falsas. La defensa, por lo tanto, debe basarse en una habilidad de diferenciar entre flujo de tráfico bueno y malo.

La solución de DDoS emplea dos sistemas que dinámicamente crea modelos de tráfico base y los compara con el flujo en tiempo real. Alguna diferencia por sobre un cierto límite dispara una alarma. Los dos sistemas están implementados en diferentes lugares en la red, dependiendo de la ubicación que mejor se ajusta a las necesidades del usuario: el dispositivo Cisco Traffic Anomaly Detector XT o el Arbor Peakflow SP de Arbor Networks, un partner del Technology Developer Program de Cisco. Arbor Peakflow SP funciona en conjunto con la funcionalidad NetFlow en el software IOS de Cisco para realizar la detección.

El Cisco Traffic Anomaly Detector XT ofrece la mayor capacidad de detección porque se sienta en el lado del cliente de la red, examinando cada flujo de tráfico mientras es entregado al cliente. Monitorea tráfico espejado desde el cableado. El tráfico es copiado por una característica basada en puertos, como el Switched Port Analyzer (SPAN), Virtual LAN (VLAN), o VPN Access Control List (VACL), o por división óptica, y el dispositivo de detección es alimentado con un stream.

El Cisco Traffic Anomaly Detector XT usa los últimos adelantos en análisis de comportamiento y



Arquitectura de la Solución de Protección de DDoS - Cisco

tecnología de reconocimiento de ataques para proactivamente detectar e identificar todo tipo de ataques DDoS. Si el detector capta un flujo anómalo, tal como un enorme y repentino tráfico hacia una dirección específica o un gran aumento de cierto tipo de tráfico, inmediata y dinámicamente genera un evento en el log del sistema, o activa un Cisco Guard remoto sobre una conexión Secure Shell (SSH) segura.

El dispositivo Arbor Peakflow SP reside en una red out-of-band, recibiendo las estadísticas del Cisco NetFlow recopiladas de varios routers en la red del proveedor de servicios. Cisco NetFlow es la tecnología de identificación de DDoS y análisis del flujo del tráfico de red para redes IP más ampliamente implementada hoy en día. Clasifica los paquetes buscando el seven-tuple en el encabezado, la información en interfaz entrante, el tipo de protocolo IP, indicador de tipo de servicio, direcciones IP de origen y destino, y puertos de origen y destino. Esta información describe un perfil del tráfico normal a lo largo de toda la red, permitiéndole a los administradores de red, ver flujos anormales mientras y donde sea que éstos ocurran. Su recopilación de datos no afecta la performance de la red o su disponibilidad, y los datos viajan fuera de la banda hacia el dispositivo Arbor Peakflow SP, para que la cobertura pueda fácilmente ser escalada en tamaño.

Haciendo uso de los datos del NetFlow, el dispositivo Arbor Peakflow SP identifica anomalías usando tanto análisis de firmas como dynamic profiling, los dos métodos más efectivos que hayan sido implementados. Los perfiles, que son continuamente reconstruidos a medida que los patrones del tráfico cambian a lo largo del tiempo, incorporan componentes temporales y topológicos para crear sofisticados modelos de comportamientos de red. Si alguna anomalía excede los límites de severidad y duración establecidos por el usuario, el dispositivo alerta al personal de la red, quienes pueden decidir si activar el Cisco Guard para detener el ataque.

Mitigación: Distracción, Limpieza, e Inyección

La función de mitigación del Cisco DDoS Protection Solution apunta a distinguir, con la mayor precisión posible, el tráfico legítimo de aquél malicioso destinado a hosts críticos (por ej.: servidores DNS, Web Servers, y softswitches de voz sobre IP), descartar el tráfico malicioso, y permitir el paso al tráfico legítimo. La mitigación se logra ya sea con un appliance Cisco Guard XT, o el Cisco Anomaly Guard Service Module, el cual reside en los switches Cisco Catalyst 6500 Series o routers Cisco 7600 Series.

Al recibir una petición del Cisco Traffic Anomaly Detector XT, el dispositivo Arbor Peakflow SP, o vía activación manual por el personal de operaciones de la red, el Cisco Guard XT envía un mensaje de Border Gateway Protocol (BGP) al router de subida, para hacer el próximo hop. El router de subida desvía el tráfico sucio (legítimo y malicioso) destinado la zona objetivo, al Cisco Guard para su limpieza. La zona es un elemento de la red protegido por el Cisco Guard contra ataques DDoS; ésta puede ser un servidor de red, un cliente o un router, un enlace de red o sub-net o una red entera, un usuario individual de Internet o compañía haciendo negocios usando Internet, un ISP, o cualquier combinación o variante de éstas.

Protección DDoS

Una vez derivado a la zona de protección, el Guard comienza a recibir el tráfico desviado y a aplicar sus políticas. Las políticas hacen referencia e instruyen al sistema de protección del Guard para que lleve a cabo una acción, la cual podría variar desde notificar al usuario de tráfico sospechoso, a direccionar el tráfico a varios mecanismos de anti-spoofing o anti-zombie del Guard o descartar dicho tráfico. Las políticas de zombis reaccionan cuando el tráfico medido excede sus límites.

Para realizar su rol protector, el Guard tiene una serie de filtros con diferentes características que son sensiblemente ajustables. Estos filtros le permiten al Guard y al usuario filtrar tráfico sospechoso y malicioso, y permitirle al tráfico legítimo pasar la zona. El Guard también tiene módulos de protección que siguen al tráfico, limpiándolo con sus mecanismos anti-spoofing. El módulo de análisis le permite al tráfico, durante la protección fluir monitoreado pero sin obstaculizarlo mientras que no se detecten anormalidades; el módulo básico tiene mecanismos anti-spoofing y anti-zombi que autentifican el tráfico; el módulo strong tiene mecanismos anti-spoofing más severos; el módulo de descarte, se deshace del tráfico malicioso; el módulo de limitación de volumen, limita el volumen del flujo de un tráfico deseado o el tráfico de una zona en general; y el módulo de reconocimiento (recognition module), el cual coordina las políticas del Cisco Guard, el sistema de filtrado, y muestrea el tráfico saliente



La Pampa se suma a la era digital
poweredbycisco.
Los gobiernos regionales que buscan la modernización de los servicios a la comunidad pueden contar con las soluciones del sector público de Cisco. Ahora más de la mitad de la población de la provincia argentina de La Pampa mejoró su calidad de vida y goza de mejor acceso a servicios de administración, educación, justicia y salud. El gobierno de La Pampa y sus habitantes están interconectados gracias a la solución de Telefonía IP de Cisco y un cableado de fibra óptica de 800 kilómetros, eliminando de raíz la barrera de las grandes distancias. Para ver cómo otros gobiernos locales hacen más productivas sus redes vaya a **http://www.cisco.com/offer/nexitpampa**
CISCO SYSTEMS
collaboration. powered by

Protección **Cisco Network Foundation**

En el clima de los negocios competitivos de hoy, conectarse a la Internet es imperativo; sin embargo, esto también expone elementos de red y su infraestructura a un sinnúmero de riesgos y amenazas. Para afrontar la creciente complejidad de los ataques en este ambiente de alta seguridad, Cisco ha mejorado las características del Cisco IOS Software (Ver NEX #19, Pág. 12) y su capacidadfuncionalidades para elementos de redes así como la infraestructura, ayudando a asegurar su disponibilidad bajo cualquier circunstancia.

Cisco Network Foundation Protection (NFP) provee las herramientas, tecnologías, y servicios que le permiten a las organizaciones, asegurar las bases de sus redes. Ésto, a su vez, permite controlar el flujo de paquetes y proteger el núcleo core de la red de un proveedor servidor de servicios de amenazas de seguridad como DDoS.

Una infraestructura segura también forma las bases de la entrega de servicios. La entrega continua de servicio requiere un enfoque metódico para proteger los diferentes planos de los router. El router está típicamente segmentado en tres planos, cada uno con un objetivo claramente identificable. El plano de datos permite la habilidad de reenviar (forward) paquetes de datos; el plano de control permite la habilidad de rutear dados datos correctamente; y el plano administrativo permita la habilidad de manejar elementos de red.

Para resguardar las bases, Cisco recomienda que los proveedores de servicio tomen el enfoque de "security toolkit", eligiendo herramientas y técnicas basadas en medir e identificar riesgos y amenazas a la infraestructura de la red. Esta caja de herramientas de seguridad debería también ser lo suficientemente flexible para que nuevas herramientas y técnicas puedan ser agregadas cuando un enfoque reaccionario de reacción es aplicado para defenderse contra una amenaza de seguridad.

Con cuidadosa consideración para cumplir con los objetivos de cada plano del router, los proveedores de servicio pueden elegir la herramienta correcta para el trabajo adecuado cuando enfrentan incidentes de seguridad.

La protección del plano de datos permite la detección de tráfico anómalo y respuesta a ataques en tiempo real. Algunas de las nuevas herramientas asociadas con el aseguramiento del plano de datos son NetFlow, IP Source Tracker, access control list (ACL) Unicast Reverse Path Forwarding (uRPF), Remotely Triggered Blackhore (RTBH) Filtering, y herramientas de QoS.

El plano de control requiere protección defensiva en profundidad para control de ruteo. Algunas de las herramientas para resguardar el plano de control son Receive ACL (rACL) y Control Plan Policing (CoPP).

El plano de administración permite administrar la infraestructura de red de Cisco IOS de forma segura y continua. Entre las herramientas para asegurar el plano de administración están el Umbral de CPU y memoria y syslog de exportación dual.

Cuando se refiere a asegurar las bases de la red, Cisco NFP debería ser considerada una medida de seguridad proactiva. Además, la segmentación metódica de los planos del router combinados con el enfoque de security toolkit, flexibilizarán y fortalecerán de gran manera y la habilidad de proveer ayuda táctica en asuntos de seguridad.

para si análisis.

El de sistema de filtro Guard y los módulos de protección operan en un modo cíclico sobre el flujo de tráfico de la zona.

Luego que el tráfico destinado a la zona atacada ha sido limpiado, el Ciso Guard permite en forma transparente que el tráfico de la zona sea inyectado nuevamente en ésta. Este estado continúa hasta que el usuario decida terminar la protección de la zona. El método de inyección depende del si la red usa un a topología core del tipo Layer 2 o Layer 3. Estos métodos, como el Policy Based Routing (PBR), Virtual Routing/Forwarding (VRF), y Generic Routing Encapsulation (GRE), son configurados en el router de bajada inmediato y en el Cisco Guard, o sólo en el Guard. Éstos se aseguran de que el tráfico limpio no regrese al Cisco Guard.

El proceso de mitigación del Cisco Guard finaliza cuando se alcanza el límite de tiempo configurable, desde que el último filtro dinámico creado para descartar tráfico DDoS haya sido quitado. Luego, el flujo del tráfico destinado a las zonas atacadas previamente ya no serán desviadas al Guard y continuarán su ruta de datos normal.

Para iniciar una zona para mitigación de DDoS, el Cisco Guard XT, al igual que el Traffic Anomaly Detector XY y el Arbor Peakflow SP, necesitan ser puestos en el modo "aprendizaje" durante tiempos sin ataques. En este modo, el dispositivo monitorea pasivamente los patrones del tráfico y sus volúmenes y límites destinados a recursos dentro de la zona, para comprender el comportamiento normal y establecer un parámetro en base al cual comparar el tráfico de la zona y ubicar anormalidades que pueda, eventualmente, convertirse en maliciosas cuando ocurra un ataque DDoS.

Modelos de Implementación

El objetivo de Cisco con su DDoS Protection Solution es permitir a los proveedores de servicio integrar los dispositivos y sus capacidades en la forma que más beneficie en costos al proveedor y a sus clientes. Hay tres modelos de implementación de servicio:

• ***Managed Network DDoS Protection:*** Los proveedores ofrecen a sus clientes protección contra ataques DDoS en sus conexiones de última milla e infraestructura de sus redes. Este modelo brinda una capa adicional que asegura la continuidad de los negocios.

• ***Managed Hosting DDoS Protection:*** Los proveedores de hosting ayudan a proteger de los ataques DDoS a servidores administrados de aplicaciones y web. La detección se lleva a cabo más cerca de los activos bajo ataque.

• ***Managed Peering Point DDoS Protection:*** Permite a los proveedores brindar conexiones libres de DDoS al por mayor a sus clientes, maximizando el ancho de banda para el tráfico legítimo.

Otra opción de implementación, es Infraestructure DDoS Protection, que les permite a los proveedores defender su propia infraestructura de red de ataques DDoS. Este modelo reduce los ataques directos en lugares vitales en la red, y protege servidores críticos en el data center del proveedor, incluyendo DNS, http, y servidores de Simple Mail Transfer Protocol (SMTP).

Además de crear nuevas ganancias, los modelos de implementación de de servicios administrados benefician a los proveedores en varios frentes. Entre ellos: mejora la visión del cliente hacia su proveedor, como un socio de confianza que entiende las necesidades de seguridad de sus negocios, potencia las capacidades de la infraestructura de red existente (por ej.: activos clave) para ofrecer el servicio con mínima inversión de capital en el costo del desarrollo.

Los beneficios a los clientes incluyen proactividad, efectividad, mitigación en tiempo real de los ataques antes de que la última milla y los recursos de los centros de datos (data centers) se vean abrumados, evitar la costosa actualización del ancho de banda de última milla debida la congestión o pérdida del tráfico causada por los ataques DDoS; y un uptime de la red mejorado para permitir la continuidad de los negocios y una satisfacción mayor del cliente. ■

Traducción realizada por NEX IT Specialist, reimpreso con permiso de Packet Magazine (Vol. 17 N°3), Copyright ©2005 por Cisco Systems Inc.

Acerca de Edmund Lamm



Líder técnico en el Grupo Ingeniería de Sistemas para Proveedores de Servicio en Cisco, se enfoca en el diseño de sistemas de seguridad administrados. Previamente a su trabajo actual, era ingeniero de marketing técnico especializado en diseño de sistemas para VoIP y MPLS VPN para proveedores de servicio.

Lecturas adicionales

• CISCO DDoS Protection Solution
Cisco.com/go/cleanpipes
• Cisco DDoS Protection Solution White Paper
Cisco.com/packet/173_8b2
• Cisco Anomaly Detection and Mitigation Portfolio
Cisco.com/packet/173_8b3

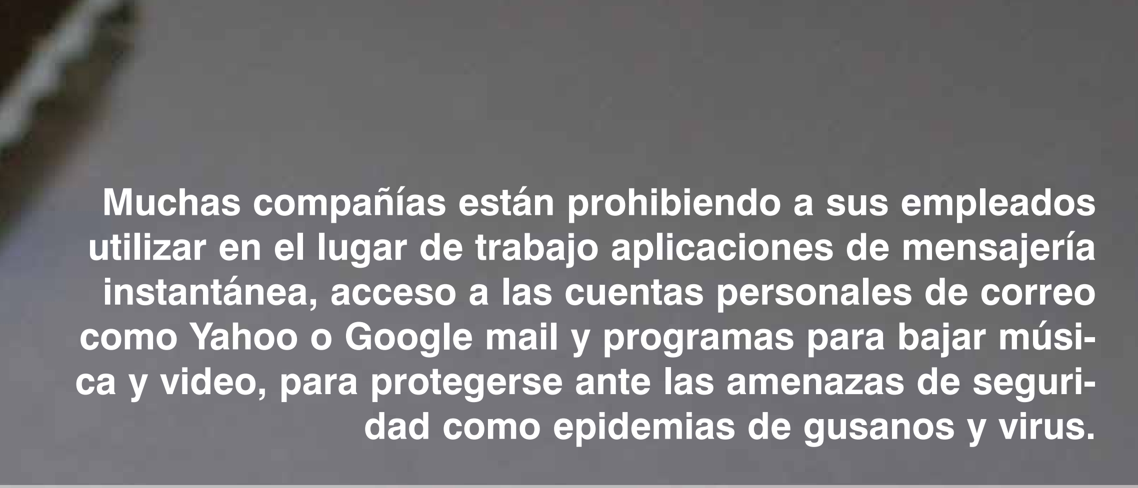
FOTO: Purdue News Service photo/Dave Umberger

Por **Gastón Tanoira**
Gerente de Soluciones de Seguridad
Cisco Systems América Latina

Seguridad Integrada contra epidemias

Gusanos y Virus

FOTO: Alejandro Cynowicz - 2006



Muchas compañías están prohibiendo a sus empleados utilizar en el lugar de trabajo aplicaciones de mensajería instantánea, acceso a las cuentas personales de correo como Yahoo o Google mail y programas para bajar música y video, para protegerse ante las amenazas de seguridad como epidemias de gusanos y virus.

Los ataques de gusanos y virus figuran hoy entre las violaciones a la seguridad más comunes en las empresas. Un servidor, un computador portátil, un PDA están expuestos a gusanos y virus en cualquier momento, y pueden propagarlos fácilmente a través de toda una organización. Infecciones como MyDoom, Blaster, Sasser, SQL Slammer, y SoBig han desestabilizado aplicaciones corporativas, web sites, bancos y aerolíneas, y han mostrado lo vulnerables que son las compañías a los ataques. Estos ataques están aumentando en severidad, velocidad y cantidad, dejando a las compañías con la necesidad de contar con mayores recursos de seguridad.

Los ataques a la seguridad pueden costarle a las compañías mucho más que las ventas perdidas o que la productividad de sus empleados. Algunos gusanos y virus pueden dejar puertas abiertas en las computadoras personales, las cuales se utilizan para robar información o usar los equipos infectados como zombies para propagar más virus, spam u otros ataques. Muchos gusanos actualmente en circulación, por ejemplo, fueron diseñados para generar ataques distribuidos de denegación de servicio (DDoS).

Por otro lado, las amenazas a la seguridad están cambiando constantemente, lo que exige a las defensas adaptarse y cambiar con ellas. En la medida en que la conectividad es cada vez mayor y el ancho de banda aumenta, la dispersión de gusanos y virus ocurre a un ritmo más veloz, complicando el problema. El gusano Blaster/Lovsan infectó a más de 1,4 millones de servidores en el mundo entero, alcanzando los 138.000 infectados a sólo cuatro horas de su liberación.

Los antivirus instalados en las computadoras personales y servidores hacen un buen trabajo previniendo gusanos y virus conocidos, pero los ataques nuevos o no conocidos (de día cero) pueden penetrar estas defensas. Por eso, tener un software antivirus es un buen comienzo, pero no resulta suficiente.

Para impedir efectivamente las alteraciones causadas por ataques de gusanos y virus, las organizaciones deben:

Contar con un sistema de identidad. La primera línea de defensa en la infraestructura de redes de una organización es determinar quién o qué está accediendo a la red, cuál es el estado del dispositivo de acceso y a qué recursos tiene derechos. Ésto permite que solamente los usuarios confiables y los dispositivos que se adhieran a las políticas corporativas de seguridad puedan conectarse a la red de una organización, enviar y recibir datos.

Proteger los End Points. Gusanos y virus atacan a las aplicaciones que corren en computadoras de escritorio, servidores y otros puntos finales de la red. Aún cuando los antivirus y los firewall son efectivos contra las amenazas con firmas reconocibles, ésto no suele ser suficiente. Hay soluciones que comprueban el comportamiento del dispositivo para identificar y prevenir comportamientos maliciosos o anómalos en los puntos finales. Es una solución que analiza el comportamiento del sistema, y que puede eliminar tanto los riesgos conocidos como los no conocidos, de acuerdo con el comportamiento de sus aplicaciones.

Controlar la Admisión a la Red. Esta funcionalidad permite habilitar el acceso a la red sólo a aquellos dispositivos finales confiables y en cumplimiento de las políticas establecidas, y restringir el acceso de los dispositivos que no cumplen con estos requisitos. Esta decisión se basa en la información existente acerca del dispositivo, como su estatus antivirus y el nivel de parches de su sistema operativo.

Limitar el contagio de la infección. Algunas veces, y a pesar de los mejores esfuerzos de una organización, un gusano o virus entra en la red. Dado que los virus y gusanos de hoy en día se esparcen muy velozmente, es necesario tener una respuesta rápida y automatizada para defenderse de ellos. Ésto sólo es posible a través de capacidades de seguridad integradas dentro de la red misma.

Encender alarmas. Sin una identificación y reacción instantánea ante la epidemia, una red puede ser derribada en minutos. Los sistemas de prevención y detección de intrusiones basados en red logran identificar, clasificar y frenar el tráfico malicioso en tiempo real y con exactitud. Una red con inteligencia apropiada puede analizar todo el tráfico que la atraviesa, reconocer un ataque, evaluar su severidad, encender las alarmas apropiadas que alerten a los administradores de la red y tomar acciones correctivas.

Segmentar la red en "islas" de seguridad. Los firewalls se usan tradicionalmente en el perímetro de la red de una organización, como puede ser una conexión a Internet, para prevenir tráfico malicioso o innecesario, o incluso impedir que los usuarios entren a la misma. Son igualmente útiles para proteger la red interior. Los firewalls pueden ser configurados para reconocer y bloquear gusanos conocidos y para bloquear puertos que no deberían ser usados en segmentos particulares de la red. Cuando se produce un ataque de gusanos o virus, los firewalls previenen la expansión de la infección por medio de la segmentación de la red interna en islotes de seguridad.

Monitorear y administrar el estado de seguridad de la red. En redes grandes y distribuidas, una visión consolidada de todos los dispositivos, de red y de seguridad, y de los servicios de seguridad permiten al equipo de IT monitorear eficientemente la red otorgándoles información en tiempo real de su estado.

Todas estas funcionalidades y medidas permiten trabajar la seguridad de redes a nivel de sistema, de manera colaborativa entre todos los dispositivos y adaptándose a las amenazas presentes y futuras.

Ataque a los datos en Argentina

De acuerdo con una investigación de Kaagan Research & Associates, el 68% de los ejecutivos argentinos afirman que los riesgos a la seguridad de datos se han incrementado en los últimos tres años. Sin embargo, menos del 35% de los ejecutivos considera que la seguridad es una cuestión de "alta prioridad".

Los incidentes relacionados con la seguridad de datos en las empresas latinoamericanas siguen aumentando, proporcionalmente al riesgo de ataques futuros, en cuanto disminuye la confianza de los ejecutivos en relación a las capacidades de poder enfrentarlos. Esta es una de las conclusiones de la encuesta "Acciones de los gerentes de IT en América Latina relativas a la seguridad", realizada por Kaagan Research & Associates, empresa de auditoría independiente y patrocinada por Cisco Systems, Inc e IBM en Argentina, Brasil, Chile, Venezuela, Colombia y México.

Qué sucede en Argentina

Según la encuesta, el 68% de los ejecutivos entrevistados en Argentina afirma que los riesgos a la seguridad se han incrementado en los últimos tres años. De éstos, el 31% cree que se han incrementado en "gran medida".

Sin embargo, sólo el 35% del top management de las empresas argentinas considera que la seguridad de datos sea una muy alta prioridad, en contraste con Colombia y Venezuela, en los que el 51% le asigna esa calificación.

El aumento significativo de los incidentes y los riesgos, contrasta con un bajo nivel de confianza en la capacidades de enfrentar ataques futuros. Apenas un pequeño porcentaje de los ejecutivos de IT entrevistados asegura que sus empresas están protegidas contra amenazas internas y externas a la seguridad. El estudio revela que sólo el 18% está "muy confiado" de que sus empresas están protegidas contra amenazas internas, en cuanto que el 23% está "muy confiado" de estar protegidas de amenazas externas.

En Argentina, el 39% de los entrevistados percibe como "muy efectivas" las funciones del Information Security, contrastando notoriamente con Brasil, en donde sólo el 9% respondió afirmativamente a la premisa.

"La encuesta reconfirma que la seguridad de los sistemas informáticos ocupa un primerísimo lugar en las prioridades de los ejecutivos de IT de Latinoamérica, dijo Gastón Tanoira, Gerente de Sistemas de Seguridad de Cisco Systems en Latinoamérica. "Sin embargo, las acciones para enfrentar estas amenazas no se corresponden con los riesgos percibidos".

"En Cisco, estamos trabajando en informar y educar sobre la necesidad de contar con una arquitectura de red que identifique, prevenga y se adapte, de manera proactiva y automática, a las amenazas a la seguridad", dijo Tanoira. La única defensa viable a los modernos ataques a la seguridad, debido a su complejidad y rapidez de expansión, es mitigar estos riesgos en la propia red. No se puede depender de dispositivos puntuales que estén en la periferia sino que la red en sí misma debe defenderse".

"Para IBM, y conforme muestra el estudio, la seguridad no es más una opción: debe estar incorporada en todo lo que hacemos. Entendemos que, para el pleno desenvolvimiento y éxito de una

empresa, la seguridad precisa permear en todos los sectores. Cada elemento de seguridad depende de una integración bien hecha con la infraestructura de IT existente. Por eso, entendemos que las soluciones, las capacidades de alcance y experiencia de IBM pueden atender de forma eficiente todas las necesidades de seguridad", destaca Roberto Cruz Arcieri, IBM Global Services Latinoamérica.

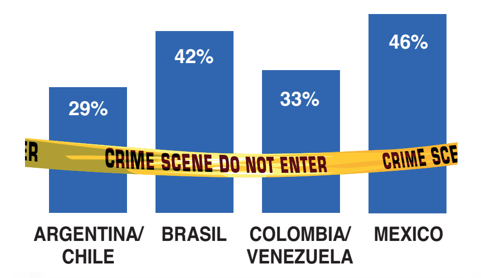
Sobre la encuesta

La encuesta "Las acciones de los Gerentes de IT de América Latina en relación a la Seguridad de la Información" fue realizada a 203 directores de tecnología y responsables de la seguridad de empresas latinoamericanas, y se llevó a cabo entre agosto y septiembre de 2005. Fueron entrevistados ejecutivos de Brasil (45), Argentina (26), Chile (25), Colombia (26), Venezuela (25) y México (56).

La encuesta involucra a empresas medianas y grandes, con un mínimo de 50 empleados. Estas empresas no son propiedad ni son controladas por una entidad extranjera.

El 57% de los ejecutivos de todas las empresas entrevistadas trabajan en empresas de más de 300 empleados y el 92% de ellos son hombres. En Argentina, el 42% de las empresas consultadas tiene menos de 300 empleados, el 31% entre 301 a 1.000 y el 23% más de 1.000.

La encuesta fue protegida, supervisada y analizada por Kaagan Research Associates, Inc., empresa analista de mercados, con sede en New York. Las entrevistas fueron realizadas por teléfono o a través de Internet, dependiendo del entrevistado. La encuesta fue patrocinada por Cisco Systems e IBM. Para reducir las posibilidades de inducción, los entrevistados no fueron informados de este patrocinio en las entrevistas.

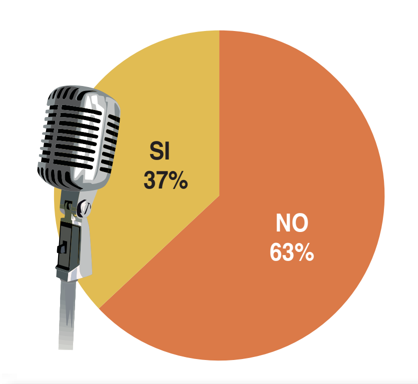


Brecha en los sistemas de seguridad de tecnologías de la información, durante el año parado

Los directores y ejecutivos de las empresas entrevistadas pertenecen a sectores corporativos más importantes y representativos de la actividad económica de la región en sus propios países, incluyendo manufacturas, servicios, bancos/seguros, distribución/minoristas, energía, minería, telecomunicaciones, agricultura y medios de comunicación/entretenimiento.

Principales conclusiones de la encuesta

Director de Seguridad de IT: Según los entrevistados, el 63% de las empresas no cuentan con un gerente o director de seguridad de IT. De éstas, el 33% planea contratar un profesional que esté a



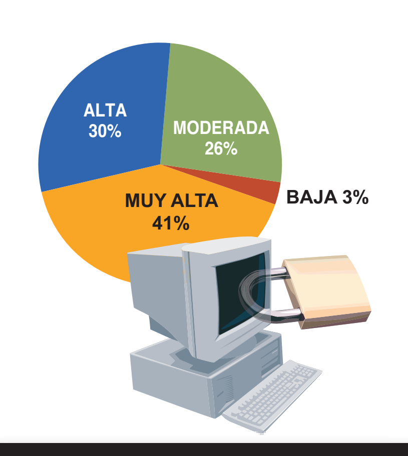
La organización entrevistada emplea un CISO o equivalente?

cargo de esta área durante los próximos dos años. Las probabilidades de tener un gerente o director de seguridad es proporcional al tamaño de la empresa: el 51% de las empresas con 1.000 o más empleados cuentan con un gerente de seguridad de IT, el 37% de las empresas con menos de 300 empleados poseen en sus filas a un gerente o director de seguridad de IT.

Presupuesto de Seguridad: El estudio demuestra que, en promedio, el 14,5% del presupuesto de IT de las empresas latinoamericanas es invertido en seguridad. Para el 66% de los entrevistados, el presupuesto aumentó en los últimos dos años, en cuanto apenas el 3% afirma que esa cantidad disminuyó en el mismo período. De los recursos destinados a la seguridad, el 51% se invierte en hardware y el 49% en software.

Incidentes de seguridad: El 38% de los ejecutivos entrevistados dice haber sufrido un ataque a la seguridad de datos durante el último año, siendo las empresas mexicanas y las brasileras las más afectadas (46% y 42% respectivamente). Según el estudio, el 61% de los incidentes relativos a la seguridad se originaron en una fuente externa. Cuanto mayor es el grado de prioridad que se le da a la seguridad de datos, menor es la posibilidad de sufrir un ataque externo, de acuerdo con los ejecutivos entrevistados.

Riesgos en la seguridad: El 63% de los ejecutivos dice que los riesgos relativos a la seguridad de datos sufrió un "aumento significativo" o "aumentó de alguna forma" en los últimos tres años. Brasil

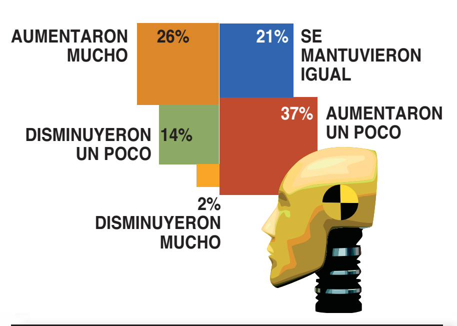


Prioridad en IS de la gerencia de la compañia

es el país en donde más ejecutivos notaron un "aumento significativo" de los riesgos en la seguridad de datos.

Confianza en la protección: Apenas un pequeño porcentaje de los ejecutivos entrevistados está confiado en que sus organizaciones están protegidas contra amenazas internas y externas a la seguridad. El estudio muestra que el 18% de los ejecutivos asegura que sus organizaciones están protegidas contra amenazas internas. La confianza en la protección contra amenazas a la seguridad decrece proporcionalmente al tamaño de la empresa: 8% de las empresas con 1.000 o más empleados asegura que sus organizaciones están protegidas contra amenazas internas, 16% en las empresas con 300 a 1.000 empleados, 25% en las empresas con menos de 300 empleados.

En relación a las amenazas externas, el 23% de los ejecutivos manifiestan que sus empresas están



Cómo cambiaron los riesgos de IS en los últimos tres años

protegidas. La confianza en la protección contra amenazas a la seguridad, también decrece de acuerdo al tamaño de la empresa. 16% de los ejecutivos de empresas con 1.000 empleados o más dijeron que sus organizaciones están protegidas contra amenazas externas; el 24% en empresas con 300 a 1.000 empleados, y el 26% en las empresas con 300 empleados o menos.

Hackers u otras amenazas: Los hackers representan la principal amenaza a los sistemas de IT, según los ejecutivos entrevistados. El estudio muestra que el 47% está "muy preocupado" por los hackers. Los ejecutivos de grandes empresas (1.000 o más empleados) son los más preocupados (61%). La segunda fuente de preocupación en lo que respecta a seguridad, son las empresas competidoras: 39% de los entrevistados dice que sus competidores son una amenaza a la seguridad de sus sistemas de IT. Este número es especialmente alto en México, donde el 52% de los entrevistados considera que la competencia como una amenaza a la seguridad. En Argentina representa el 35%.

Desafíos relacionados a la seguridad: Las limitaciones de presupuesto son el principal desafío que los ejecutivos de IT enfrentan en cuanto a la seguridad de datos. Para el 80% de los entrevistados, el presupuesto es un problema. Para el 42% de los entrevistados, es un "gran problema", y para el 32% es un "problema menor". El segundo desafío más importante que enfrentan los ejecutivos de sistemas de seguridad, es concientizar a los directores de las empresas sobre el valor de la seguridad de IT (68% de los entrevistados). ■

Soluciones de seguridad en Redes

Federico Chaniz
Bussines development manager
Softnet Logical

La implementación de firewalls y redes privadas virtuales no garantiza, en la actualidad, un resguardo total frente a las amenazas informáticas. Por eso, crece la necesidad de contar con herramientas más avanzadas que permitan defenderse mejor frente a agresiones cada vez más especializadas y difíciles de detectar. Además, la epidemia del spam y la masificación de las redes inalámbricas generan nuevos desafíos.

Clásicos

Durante los 90 fue norma la instalación de Firewalls y Antivirus. A principio del 2000 las soluciones de VPN para segurización de acceso remoto eran la tendencia del momento. Actualmente cerca del 100% de las empresas tienen implementadas soluciones de Firewalls y 80% de las mismas tiene soluciones de VPN. Estas soluciones cuentan con una amplia aceptación en el mercado, pero están lejos de proteger a los usuarios de las amenazas que actualmente se encuentran en las redes de comunicaciones.

En general, los Firewalls no dejan de ser "puertas" en los puntos de accesos de la red, que pueden abrirse o cerrarse a nivel de red (Nivel 4, OSI) pero no "miran" quien está entrando; o sea que su análisis del tráfico cursado no llega a nivel de aplicación (Nivel 7, OSI).

Las Redes Privadas Virtuales (VPN) son en realidad una manera de "privatizar" las comunicaciones sobre rede publicas, pero lejos están de segurizar el contenido transmitido por este vinculo privado virtual. Salvo que se implemente sobre las mismas soluciones de encripción tipo DES, que de todas maneras son comunes en este tipo de soluciones.

IDS/IPS

En los últimos años el mercado tomó conciencia de la necesidad de protección mediante herramientas más complejas que permitan una mejor defensa ante ataques cada vez más especializados y difíciles de detectar que explotan las vulnerabilidades de redes y aplicaciones. Es así como las soluciones de IDS e IPS han cobrado fuerza, si bien actualmente sólo el 50% de las empresas han adoptado su utilización. Muchas marcas líderes del mercado han centralizado su estrategia en potenciar estas soluciones y hacerlas cada vez más complejas y eficientes a la hora de proteger las redes de sus usuarios.

El termino "firmas" es ya parte del lenguaje común en el ambiente de seguridad, y no son ni más ni menos que patrones de tráfico malicioso, identifi-



cado por los fabricantes, e incluidos en sus soluciones como un parámetro de comparación del tráfico analizado (ahora sí a Nivel 7 OSI) para de esta manera hacer más "profundo" el análisis y la detección. La calidad de estas soluciones, de las muchas ofertas existentes en el mercado, está dadas básicamente por los siguientes parámetros:
- Cantidad y calidad de estas "firmas"
- Tiempo de respuesta para generar nuevas "firmas", a partir de nuevos patrones maliciosos.
- La proactividad para estudiar vulnerabilidades y generar "firmas" antes de la generación del ataque.

Sin olvidar por supuesto la siempre presente performance del equipo (latencia), ya que el estudio de la totalidad del tráfico de red, su comparación con patrones, y la toma de desiciones crea un cuello de botella en el flujo de información, que debe ser considerado dentro del análisis de soluciones. No siempre la solución mas confiable de IDS/IPS será la más "performance", y viceversa.

"Las Redes Privadas Virtuales (VPN) son en realidad una manera de "privatizar" las comunicaciones sobre rede publicas, pero lejos están de segurizar el contenido transmitido por esté vinculo privado virtual"

Spam!

Estas soluciones si bien detienen la mayoría de los ataques que llegan a través de la red, otras amenazas específicas requieren atención especial y soluciones a medida. La "epidemia" del spam llega a generar 50% del tráfico de mail no deseado y afecta a todos los usuarios de correo electrónico. Soluciones que detienen este tipo de ataques que degradan la performance de la red y aplicaciones, se hacen cada vez más necesarias y su implementación ha comenzado a masificarse en los últimos tiempos.

Desde soluciones "open source" que permiten desarrollar plataformas de antispam con reglas propias y "manuales" muy difundidas actualmente; hasta fabricantes con "bases de conocimiento" propias, que cataloga la "reputación" de cada uno de los "remitentes" de mail y permite un grado de filtrado del spam realmente muy preciso. Esta precisión no es menor, el temido "falso positivo" (un mail bueno catalogado como spam, y por lo tanto descartado) es el dolor de cabeza de los implementadotes de este tipo de soluciones.

Por supuesto que varias de este tipo de soluciones vienen en formato "appliance", con sus propios procesadores, almacenamiento y MTA. No olvidemos la performance!. Fabricantes específicos de este tipo de soluciones han cobrado nombre en los últimos tiempo y amplían y mejoran su oferta de soluciones día a día, para este "flajelo".

Wi-Fi también

La masificación y aceptación de las redes Wireless y las ventajas de conectividad instantánea que la misma genera, han planteado una revisión de los esquemas de seguridad en este tipo de redes, donde la autenticación de los usuarios y la seguridad de los datos trasmitidos en estos medios "abiertos", fácilmente accesibles y vulnerables en un principio, ha llevado al desarrollo de nuevos estándares de autenticación y encripción de los datos.

El usuario, accediendo a una red Wi-Fi puede "abrir" una VPN contra su Host y de esta manera segurizar su conexión inalámbrica (siempre y cuando no este bloqueada la aplicación en la red de acceso). Pero qué pasa con las empresas que implementan sus propias redes corporativas Wi-Fi? Y con los proveedores de servicio que brindan acceso pago? El gran "temor" es que usuarios no habilitados ingresen en la red, no sólo para usarlas, eso sería lo de menos.

Y no alcanza con implementar calves de acceso encriptadas (WEP) para los usuarios, son fácilmente hackeables, y todos saben como hacerlo. La gran panacea es que las redes Wi-Fi puedan tener el mismo nivel de seguridad que las redes cableadas. Se pretende que sobre una red Wi-Fi pueda implementar DNS, VLAN, QoS, etc; como en cualquier switch de Layer 3 de LAN. Sin que sea masivo, ni mucho menos, los fabricantes (de networking) han rápidamente desarrollado soluciones de seguridad específica para este problema y permiten en la actualidad que ésto sea posible.

Inteligencia Artificial

La complejidad de las arquitecturas de las redes de comunicación, no sólo en el ámbito de los proveedores de servicio sino en empresas, cuya estructura se asemeja bastante, ha hecho que sea necesario el desarrollo de soluciones que puedan dar una visibilidad global a la red, a estudiar su "comportamiento" en general y a detectar anomalías en el mismo manera "inteligente" y "automática".

Existen herramientas que han podido llevar a la realidad esta necesidad y ofrecen soluciones con este nivel de análisis de red. Appliance específicos que tienen la capacidad de "aprender" solos cuál es el comportamiento normal de una red, incluso a nivel de usuario; conociendo por ejemplo que tipo de aplicaciones usa cada uno, con cuales host o computadoras se comunica más frecuentemente, cuál es el volumen de tráfico que trafica, etc. Una vez aprendido ésto, sólo es cuestión de detectar cualquier cambio en lo que se considera normal, y avisar al operador. En este tipo de soluciones, la toma de acciones de manera automática no es recomendada, ya que la anormalidad del tráfico no necesariamente significa su maliciosidad ni que deba ser eliminado.

La correlación de eventos es otro tipo de solución que brinda a las redes cierta "inteligencia" no para detectar eventos (logs), sino hacer comparaciones entre ellos y sacar una "conclusión" respecto de lo que verdaderamente está pasando. Lo interesante en estas herramientas de correlación es que las mismas no están diseñadas para interpretar y relacionar eventos de un mismo fabricante; sino que actualmente existen herramientas "independientes" que toman información de equipos de seguridad de distintas marcas para luego hacer un análisis de lo que está pasando en la red.

"El termino "firmas" es ya parte del lenguaje común en el ambiente de seguridad, y no son ni mas ni menos que patrones de tráfico malicioso, identificado por los fabricantes"

Conclusión

Este complejo escenario en el tema seguridad, incluso luego de esta simplificación, ha hecho que una solución completa e integral no dependa sólo de la adopción de una solución específica sino probablemente de la integración de varias soluciones y tecnologías de diferentes fabricantes. Y esta integración deberá tener en cuenta no sólo la manera en que se complementan, sino como interactúan entre ellas, cómo optimizan su funcionamiento, y cómo se controlan de manera integrada. ■

El factor humano, una de las principales amenzazas informàticas.

Alrededor del la mitad de las infecciones de PCs y redes son evitalbles, dado que suelen ocurrir como consecuencia del accionar de internautas distraídos, no informados o curiosos que colaboran inconscientemente con los atacantes. ésta fue la principal conclusiòn de un relevamiento llevado a cabo por Trend Argentina, empresa especializada en seguridad informàtica.
De acuerdo al estudio, el 50% de las 15 principales amenanzas detectadas durante 2005 corresponden al llamado grayware. Se trata de programas con còdigos malicioso que funcionan de forma encubierta, brindando al usuario alguna utilidad o licencia, al que accede sin darse cuenta. Asì, los mismos afectados colaboran en la propagaciòn de virus. El hecho de que el factor humano sea tan importante a la hora de adquirir infecciones, implica que cualquier estrategia de seguridad debe combinar en forma adecuada no sólo soluciones ajustadas a las necesidades particulares de cada empresa, sino tambièn la capacidad constante del usuario mediante seminarios y jormadas asistenciales.

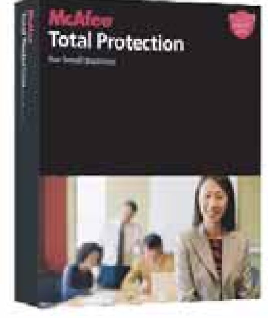
Se puede ir en muchas direcciones

ANTI-VIRUS
INTRUSION PREVENTION
NETWORK ACCESS CONTROL
ANTI-SPYWARE
FIREWALL
ANTI-SPAM

Nosotros podemos guiarlos hacia una solución integral

McAfee® Total Protection™

McAfee® Total Protection™ (ToPS) para PyMES. Seguridad siempre actualizada en una única solución.



McAfee® Total Protection™ es una solución integral de seguridad para PyMES que proporciona la protección más amplia contra todo tipo de amenazas, sean virus, spyware, spam, phishing, ladrones de identidad o hackers.

McAfee® Total Protection™ para PyMES simplifica la seguridad y propociona una completa protección para estaciones, servidores y correo electrónico.

www.mcafee.com
011-4326-5115



Google™ Como herramienta de ataque.

Pedro Paixao
SE Manager (Security Expert Manager)
Check Point

“Las fuentes de información públicas, como los buscadores, permiten a quienes lo deseen, acceder al menos al 80% de la información de nuestras redes, sin la necesidad de exponer su identidad”

Tal vez un día se diga que si pasó en la vida real, está publicado en algún sitio de Internet. Puede que todavía no estemos a ese nivel, pero es indiscutible que la cantidad de información, hoy publicada en Internet, es de tal orden que el problema principal es encontrar lo que uno desea, de una manera rápida y relevante. Con esta necesidad nacen algunas de las mayores empresas del mundo, como Yahoo y Google, y otras ya establecidas, como Microsoft, e invierten billones de dólares para dominar esta importante tecnología: la búsqueda de información.

Las grandes inversiones trajeron muchas mejorías en los resultados obtenidos, y nuevas tecnologías como Tagging y Web 2.0 prometen aumentar el contexto y la información semántica de la Web y con ello llevar la búsqueda de información a un nuevo umbral de calidad.

Los motores de búsqueda se transformaron en las puertas de entrada a Internet y la realidad de hoy es que si un sitio no está publicado en un motor de búsqueda, o no aparece en los primeros resultados obtenidos por el usuario, la probabilidad de que sea visitado es muy baja.

Mucho del trabajo que hacen los motores de búsqueda es navegar por Internet en busca de nuevos sites, o nueva información, que una vez encontrada es almacenada e indexada. Genéricamente se llama a la aplicación de indexación el searchbot, y en el caso de Google éste se conoce como el GoogleBot.

El GoogleBot es un proceso automático, con una capacidad de indexar millones de páginas web y otros documentos a cada segundo. Una vez indexada la información está disponible para todos los usuarios que la busquen. Como en muchas otras tecnologías, existe un lado bueno y un lado oscuro, y aquí empieza el interés del punto de vista de seguridad.

En este artículo hablaré de algunas técnicas que permiten identificar vulnerabilidades, hacer análisis de seguridad o mismo penetration testing, utilizando nada más que un web browser y Google. En 2004 se reportó el primer gusano de Internet que utilizó estas técnicas para identificar sus víctimas y así propagar su código malicioso. Muchas de ellas pueden ser utilizadas con otros motores de búsqueda, y su simplicidad y poder es sorprendente.

Debido a que algunos de los datos presentados son reales, los hosts y otra información personal fueron ocultados. También como nota me gustaría decir que ningún web site fue visitado directamente para obtener los datos presentados, todos ellos fueron conseguidos accediendo solamente a Google, su cache o su conversión de documentos a HTML.

Comandos Avanzados

Mucho mas allá de las tradicionales búsquedas ejecutadas por la gran mayoría de los usuarios, tenemos la posibilidad de pedir a Google que nos presente resultados más relevantes, o interesantes, utilizando la página de búsqueda avanzada, o mas fácil todavía, utilizando los comandos avanzados en la página de búsqueda simples. [fig.1]

Utilización básica:

• El uso de comillas “ “ busca toda la string, por ejemplo “operadores avanzados” sólo devuelve resultados que contengan exactamente esta string

• Utilizar ‘+’ para palabras esenciales, por ejemplo +password sólo retornan resultados que contengan la palabra “password”

• Utilizar ‘-‘ para palabras no deseables, por ejemplo "Bill Gates" –microsoft, retorna todos los documentos que contengan la string “Bill Gates” pero no Microsoft.

Google Advanced Search — Advanced Search Tips | About Google

Find results: with **all** of the words / with the **exact phrase** / with **at least one** of the words / **without** the words — 10 results — Google Search
Language: Return pages written in — any language
File Format: Only — return results of the file format — any format
Date: Return web pages updated in the — anytime
Occurrences: Return results where my terms occur — anywhere in the page
Domain: Only — return results from the site or domain — e.g. google.com, .org More info
Usage Rights: Return results that are — not filtered by license — More info
SafeSearch: No filtering / Filter using SafeSearch

Page-Specific Search
Similar: Find pages similar to the page — Search — e.g. www.google.com/help.html
Links: Find pages that link to the page — Search

[fig.1] Ciclo de vida de un proyecto de data warehouse

Operadores avanzados

Ver cuadro en esta página.

Operador	Descripción	Ejemplo
site:	Restringe la búsqueda al dominio DNS en cuestión	*site:www.microsoft.com*
related:	Devuelve todas las páginas que Google encuentra relacionadas con la URL utilizada	*related:www.cnet.com*
link:	Devuelve todas las páginas que Google conoce y que conectan a la URL utilizada	*link:www.checkpoint.com*
phone:	Intenta buscar el número de teléfono para el nombre mencionado	*phone:"John Smith"*
filetype:	Sólo retorna archivos del tipo indicado, si es utilizado con '-' no retorna archivos del tipo indicado	*filetype:mp3*
detrange:	Devuelve resultados que fueron indexados en una fecha, o entre dos fechas. La fecha tiene que estar en formato Juliano, o sea el numero de días que pasaron desde Enero, 1 de 4713 A.C.Utilizar un conversor de fechas para este operador	*detrange: 2453857-2453882 Busca entre 1 de Mayo de 2006 y 26 de Mayo de 2006*
inurl:	Devuelve resultados que contengan la string indicada en la URL	*inurl:admin*
intitle:	Devuelve resultados que contengan la string indicada en el título de la página	*intitle:confidential*
intext:	Devuelve resultados que contengan la string indicada en el texto de la página	*Intexto:confidential*
allinurl:	Devuelve resultados que contengan todas las strings indicadas en la URL	*allinurl:admin config*
allintext:	Devuelve resultados que contengan todas las strings indicada en el texto de la página	*allintext:confidential "do not distribute"*
allintitle:	Devuelve resultados que contengan todas las strings indicadas en el título de la página	*allintitle:confidencial interno*
*	Se pueden utilizar comodines para representar palabras no para completarlas	*"username=* password="*
nnn..mmm	Rango decimal, pude ser utilizado para buscar números	*1000..9999*

La Máquina del Tiempo

Una de las características más importantes de todos los motores de búsqueda es que éstos no buscan directamente la web, sino que buscan una representación de la web como fue vista por el Searchbot en un dado momento en el tiempo. Esta información es almacenada y puede que esté completamente desactualizada. Este aspecto de la tecnología tiene implicaciones más o menos importantes desde el punto de vista de seguridad.
Como ejemplo tomemos una empresa que, por alguna razón, publica documentos confidenciales en su servidor web, pensando que sólo sus clientes tienen acceso a los mismos. Dentro de días se enteran que debido a un problema de configuración los documentos están disponibles para todo el mundo. El webmaster se apura a reconfigurar el servidor, y todo está funcionando como planeado. ¿Pero lo estará realmente?
En la realidad el GoogleBot indexo el sitio web y ahora todos los documentos están almacenados en la cache de Google. Un hacker busca:
Google Search: *site:compania.ar filetype:pdf*
Y recibe la lista de todos los documentos. Como estos links ya no son válidos, podemos utilizar la opción "View as HTML" para tenemos acceso al contenido. [fig.2]
Otra opción sería utilizar el link "Cached" [fig.3]
Para búsquedas en el tiempo más avanzadas, se puede utilizar el operador detrange:.
Las implicaciones de ésto son tremendas y Google brinda métodos de borrar información de su Cache, pero le corresponde al dueño de la información pedir que sea removida. http://www.google.com/webmasters/remove.html

El Proxy Transparente

Como vimos en los ejemplos anteriores es posible ver el contenido de páginas web u otros documentos sin entrar a los sitios que los publican utilizando las opciones "View HTML", y "Cached" de Google. Esta característica es muy útil para hackers pues pueden investigar todo el sitio de sus victimas, sin nunca tener que entrar a sus servidores!
Se podría llamar a estas funcionalidades el Proxy Google, pues permite, sólo con el acceso al sitio de Goolge, "entrar" al sitio de terceros. Otra forma importante de Proxy vía Google se consigue cuando uno utiliza sus servicios de traducción automática. [fig.4]
Ejemplo: Yahoo.com vía Google Translation Services, Yahoo.com ve un acceso de Google no del cliente que la pidió. [fig.5]

Configuraciones Default

Desafortunadamente la mayoría de las aplicaciones presentan problemas de seguridad en sus configuraciones estándar, o default. El conocimiento de versiones, y configuraciones es muy importante una vez que se pueden buscar bases de datos de vulnerabilidades y rápidamente identificar victimas.
Por ejemplo podríamos utilizar lo siguiente para



[fig.2]
[fig.3]
[fig.4]

identificar instalaciones default de Apache:
Google Search: *intitle:"Test Page for Apache" "It Worked!"*
Otra técnica muy simple que brinda excelentes resultados en servidores con PHP es buscar archivos generados por phpinfo. Todas las distribuciones de PHP incluyen la función phpinfo() que cuando es ejecutada enlista toda la configuración del servidor en una sola página. Así podríamos hacer:
Google Search: *intitle:phpinfo*
Y obtener unos 100,000 resultados, como el que se ve en la figura 6.

Exploits

La costumbre era ver a los hackers como gente muy inteligente con la capacidad, y conocimiento suficiente para investigar problemas en protocolos, sistemas operativos o aplicaciones, y desarrollar maneras de explotarlos para con ello tener acceso a información o recursos informáticos. Ésta era una comunidad restricta y de difícil acceso. La información circulaba en un sub-mundo al cual, para pertenecer, era necesario tener el merito suficiente. Hoy existen docenas de sitíos web donde se listan todas las vulnerabilidades conocidas y como explotarlas. O sea ya no es necesario conocer a fondo la tecnología de ataque, es suficiente saber como encontrar los programas que explotan una vulnerabilidad, o exploits del inglés, y utilizarlos contra aplicaciones vulnerables.
Podemos así separar la tarea de atacar una víctima en 3 fases: encontrar una vulnerabilidad, encontrar un exploit y encontrar una victima. En todas ellas Google puede ayudarnos.
Una simple búsqueda de "bugtraq" y "inurl" nos revela todas las vulnerabilidades listadas en Bugtraq, una lista de correo donde se publican problemas de seguridad, que contengan la palabra "inurl".
Google Search: *bugtraq inurl* [fig.7]
Siguiendo el primer link podemos ver una vulnerabilidad del Woltlab Buletin Borrad.
Ya tenemos la vulnerabilidad. Más abajo en el texto, podemos ver como explotar la vulnerabilidad reportada; Ya tenemos el exploit. [fig.8]
Como ya es práctica común, se listan también ejemplos de cómo buscar en Google las aplicaciones afectadas, lo único que tenemos que hacer es utilizarlos, y ya tenemos las víctimas. ¡Todo en 30 segundos o menos! [fig.9]

Bases de Datos

Para los que están acostumbrados con el desarrollo, o configuración de aplicaciones web, sería impensable publicar la base de datos directamente en el servidor web, sin autenticación y disponible a todo el mundo. Para evitar el acceso directo a la información se instalan firewalls, colocando los servidores involucrados en DMZs distintas, se configuran sistemas de autenticación, se programa la lógica necesaria para que sólo la información deseada sea visible a los usuarios con los privilegios correctos, y muchas veces se usan mecanismos de encriptación de todas las



[fig.5]



[fig.6]



[fig.7]

```
GPC
GET ->
http://[victim]/[WBBDir]/info_db.php?action=file&subkatid=1&noheader=1&fileid=-1/**/[SQL/XSS
EXAMPLE ->
http://[victim]/[WBBDir]/info_db.php?action=file&subkatid=1&noheader=1&fileid=-1/**/UNION/**
```

[fig.8]

```
http://www.nukedx.com/?getxpl=17
---
Dorks: inurl:info_db.php , inurl:/wbb2/info_db.php , inurl:/board/info_db.php,
inurl:database.php , inurl:/wbb2/database.php , inurl:/board/database.php
allintext:Datenbank Trooper WbbCoderForum.de etc. etc.
---
```

[fig.9]

sesiones. Todo este trabajo está perdido con un archivo de backup, o SQL, un sencillo mensaje de error de la aplicación, o una exportación de datos. Todo lo que necesita el hacker es un simple motor de búsqueda, sin siquiera acceder al site victima!

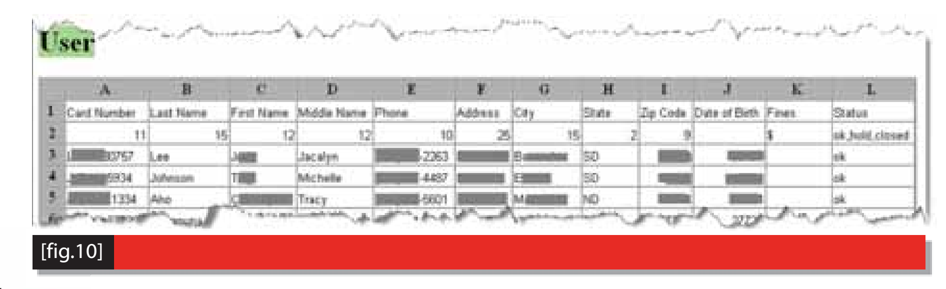
Muchas veces la información contenida en la base de datos se originó en archivos Excel, o los operadores la exportan a este formato para facilitar la creación de reportes, estadísticas, u otras manipulaciones. Algunas veces estos archivos quedan en el servidor web, en una carpeta "escondida" esperando que el Googlebot los indexe. Lo suficiente para comprometer toda la información de la base de datos. Veamos un ejemplo: vamos buscar todos los archivos Excel (filetype:xls) que contengan uno de los nombres más comunes del Inglés "Davis", y que además contengan también la palabra "User".

Google Search: *filetype:xls Davis User*

Uno de los resultados, accedido vía Google Cache, es una base de datos de una biblioteca que contiene la información de centenas de miembros, sus números de tarjeta, teléfonos, direcciones y hasta cuánto dinero deben a la organización. [fig.10]

Otra posibilidad es buscar por mensajes de error comunes a los sistemas de bases de datos que revelan demasiada información. Por ejemplo:

Google Search: *"ASP.NET_SessionId" "data source="*



[fig.10]



[fig.11]

Revela, como siempre, miles de sites que generaron en algún momento mensajes de error de Active Server Pages (ASP) cuando se intentaba conectar a la base de datos. Uno de ellos es muy interesante dado que la página, almacenada en Google Cache, habla de la política de protección de datos, en todas sus formas por la organización dueña del site, y más abajo se pueden ver las contraseñas de las bases de datos utilizadas – como mínimo irónico. [figs.11 y 12]

[fig.12]

Utilizando el conocimiento del sistema de base de datos utilizado es posible buscar por nombres de funciones comunes, en archivos de "include" que muchas veces no son procesados directamente por el servidor web. Un ejemplo típico de ésto son los archivos .inc utilizados en PHP. Al contrario de los archivos .php que son procesados por el servidor web antes de ser enviados hacia el cliente, los archivos .inc son muchas veces enviados sin procesamiento y con ello revelan todo el código fuente que contienen. Este tipo de archivo tiene que estar disponible para lectura por el servidor web, pero no para el acceso directo por parte del cliente remoto. El problema es que mensajes de error revelan links para estos archivos, o las carpetas donde están almacenados permiten su listado completo, y como tal ellos pueden ser indexados por Google. Si buscamos por todos los archivos .inc (filetype:inc) que contengan la función de MySQL mysql_connect(), vamos a tener algunas sorpresas:

Google Search: *filetype:inc mysql_connect() –cvs*

No queremos los resultados que contengan la palabra cvs pues ésta se encuentra en repositorios de software libre que van a generar muchos "falsos positivos". [fig.13]



[fig.13]


LICENCIAS
ON LINE
www.licenciasonline.com


Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

En este ejemplo podemos ver dos sitios en que el usuario y contraseña de MySQL aparecen directamente en el resumen del documento, ni siquiera tenemos que visitar la página en cache!

Otro ejemplo que podemos mencionar es la búsqueda por comandos SQL. Cuando se instalan las aplicaciones y se crean las bases de datos es necesario utilizar archivos de texto con comandos SQL, que una vez procesados deberían ser borrados, y removidos del servidor, pero una vez más el operador despreocupado nos hecha una mano. [fig.14]

Google Search: *"DROP TABLE IF EXISTS"*

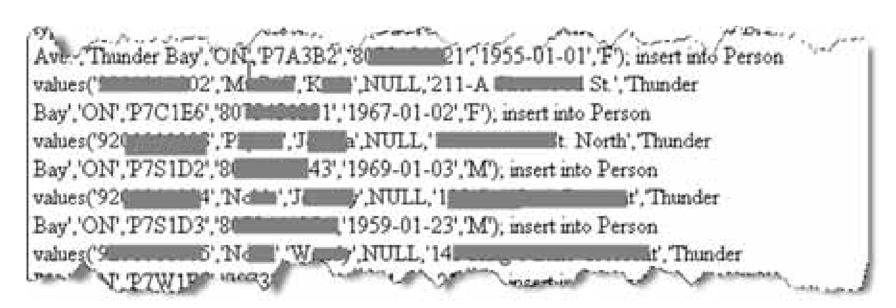
individually dropping each table (somewhat but not exactly similar ...
.com/doc/mysql/en/drop-table.html - 14k - Cached - Similar pages

drop table if exists Person; drop table if exists Patient; drop ...
drop table if exists Person; drop table if exists Patient; drop table if exists MedicalWorker; drop table if exists Clerk; drop table if exists Doctor; ...
.ca/~siddiqui/MedFclty.txt - 15k - Cached - Similar pages

drop table if exists 'word_types'; create table 'word_types ...
Antonyms.txt' into table antonym; drop table if exists copyrights; create table copyrights (copyright TEXT) TYPE=MyISAM; insert into copyrights values ...

[fig.14]

Se miramos el Cache podemos ver la estructura de la base de datos e información personal que quedó en archivo de texto, libremente accesible. [fig.15]


Ave.','Thunder Bay','ON','P7A3B2','80 21','1955-01-01','F'); insert into Person
values(' 02','M ','K ','NULL','211-A St.','Thunder
Bay','ON','P7C1E6','80 1','1967-01-02','F'); insert into Person
values('92 ','P ','J a','NULL',' t. North','Thunder
Bay','ON','P7S1D2','8 43','1969-01-03','M'); insert into Person
values('92 4','N ','J ','NULL','1 t','Thunder
Bay','ON','P7S1D3','8 ','1959-01-23','M'); insert into Person
values('9 5','N ','W ','NULL','14 t','Thunder

[fig.15]

FTP Access

No es tan común que webmasters dejen en sus servidores web, los archivos de configuración de sus clientes FTP pero, como ya vimos en los párrafos anteriores, lo esperado y lo real es muy distinto. Una simple búsqueda de archivos .ini (filetype:ini) que contengan "ws_ftp" y "pwd", revela muchos sitios, y uno de ellos escogido al azar del Cache contiene docenas de servidores ftp, los nombres de usuario, y la contraseña.

Googel Search: *filetype:ini ws_ftp pwd* [fig.16]

sndts=H:\public_html\geral\WS_FTP\complete.wav sndtf=H:\public_html\geral\WS_FTP\error.wav
soundflags=8 BELL=1 usewave=0 [progene] HOST= UID=www PASVMODE=1
TIMEOFFSET=0 ldir0=H:\WS_FTP
PWD=VCD51DD9D12ABBA14EB882F70ABC75267776AA3952C6CA0 [FIREWALL]
HOST= 4 UID=www FIRETYPE=1 PORT=21
PWD=V9A4C3F59FCDEE70EFB96F8A7F93D224BAD67A2675B6E9C71 [biogene]
HOST=ftp. .br UID=www.biogene.ind.br
PWD=V19FD6D2D6CF4BDE6E7B83ABBBA1585BFA47A3B3B8171 PASVMODE=1
TIMEOFFSET=0 rdir0="/bd" rdir1="/" rdir2="/site/governo" rdir3="/site" rdir4="/site/biogene"

[fig.16]

Estas contraseñas pueden ser fácilmente descifradas utilizando herramientas libres que puedes buscar con… Google, claro!

Ahora lo único que el hacker tiene que hacer es conectar al servidor ftp con estas credenciales y quien sabe lo que va encontrar ahí.

Otras Posibilidades

El potencial de las técnicas presentadas es casi ilimitado y con alguna imaginación se puede pensar en muchas otras búsquedas que van a revelar información importante.

• Buscar servidores VNC
- **Google Search:** "VNC Desktop" inurl:5800
• Buscar libros electrónicos
- **Google Search:** *filetype:lit lit (books|ebooks)*
• Outlook files
- **Google Search:** *outlook filetype:pst*
• Listado completo de carpetas
- **Google Search:** *intitle:index.of "parent directory"*

Evitando Problemas

La mejor manera de evitar este tipo de problemas es la prevención, no dejar archivos de backup en el servidor web, no dejar configuraciones default, configurar la autenticación correctamente, y es muy importante configurar el robots.txt. Los searchbots de los motores de búsqueda respetan el Robots Exclusión Standard o robots.txt protocol (www.robotstxt.org), que no siendo un estándar formal, es una convención creada en 1994, que permite a los webmasters decidir que partes de sus sitios web no son indexadas.

El archivo robots.txt debe existir en la raíz del sitio web (ejemplo http://misitio.com.ar/robots.txt) y su contenido se resume normalmente a un conjunto de líneas de texto con el comando Disallow: seguido de la carpeta que deseamos que no sea indexada.

Ejemplo:

```
User-agent: *
Disallow: /cgi-bin/
Disallow: /images/
Disallow: /tmp/
Disallow: /private/
```

Si en vez de carpetas completas se desea evitar que una página sea indexada se debe utilizar el Meta Tag ROBOTS

<META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW">

Atención que no todos los searchbots respectan este tag.

Si después de todos los cuidados, nuestro site todavía aparece en el índice de Google debemos pedirles que lo retiren. Este proceso puede ser hecho en forma manual o automáticamente, si el servidor web retorna un error "404 Not Found". Todos los documentos con error 404 son removidos del índice automáticamente. El problema con este abordaje es que no tenemos control de cuando el documento va ser retirado del índice, si deseamos tener este control hay recurrir al proceso manual vía http://www.google.com/webmasters/remove.html

Si no conoces lo que está publicado en nuestro sitio web otros lo conocerán, todo gracias a Google y sus compañeros. ■

Cómo funciona un laboratorio de

Detección de Malware

Panda Software

Cada vez más Internet está presente en la vida de los individuos y de las compañías, y todos los elementos positivos y negativos de la sociedad se han trasladado a ella, no podíamos pensar que el delito no lo fuese a hacer, pero lo visto y escuchado, conforman una realidad mucho más espeluznante de lo que uno supone.
El Crimeware es una realidad y para defenderse no alcanza con la tecnología que tengamos instalada en nuestros PCs, sino en la responsabilidad de estar informados de esos riesgos y del buen funcionamiento de centros de investigación y desarrollo como Panda Labs.

Nuestra huella digital no es aceptada por el sensor que abre las puertas de Panda Labs, uno de los laboratorios más modernos e importantes de la industria de la seguridad. La pregunta inicial nació sola, para qué tanta seguridad? Unas horas después cuando salíamos, estaba más que claro. Pero comencemos por el principio. Cómo funciona, qué tareas se llevan a cabo, qué se detecta y cómo interactúa con el resto de la industria y con la comunidad en general es lo que trataremos de describir a continuación gracias a la entrevista exclusiva que Luis Corrons, su director, le ofreció a Nex IT, en la visita, donde nos comenta que "El malware ha cambiado, ya no busca epidemias masivas y sonoras. Hoy el malware se orienta al delito, lo que hace que quien delinque no desea reconocimiento y fama como antes, ahora necesitan trabajar en las sombras lo que hace mucho más difícil detectar el malware". Nuestra visita estará llena de ejemplos de una realidad que asusta, con casos que se pueden divulgar y otros que no, ya que trabajando en conjunto con Interpol, FBI, y Policías locales están en etapa de investigación. (Ver recuadros aparte).

En un laboratorio sin tubos de ensayo, hay varias cosas que saltan a la vista, mucha más gente trabajando que la que esperábamos ver, cada uno con dos pantallas, plasmas en las paredes reflejando el estado mundial del malware, columnas decoradas con los nombres de los más famosos malwares, como para no olvidarse quién es el enemigo, relojes con las horas de varios puntos del planeta, pues en Panda Labs, no se duerme, y alarmas visuales y auditivas que alertan al personal cuando la muestra analizada posee un grado de peligrosidad importante. El proceso de detección de malware comienza así:

Al laboratorio le llegan muestras desde varios orígenes, a través de Honey Pots, que Panda Labs hoy tiene en USA, China, Inglaterra, España, y próximamente en Latino América, siendo Argentina uno de los candidatos a ello. A través de sistemas de monitoreo mundial, de muestras que envían los clientes de todo el mundo, del intercambio de colecciones que se realizan con otras compañías de la industria y de foros de seguridad, desde hace 2 años, las tecnologías TruPrevent desarrolladas por Panda Software se han constituido como la principal fuente de detección de malware.



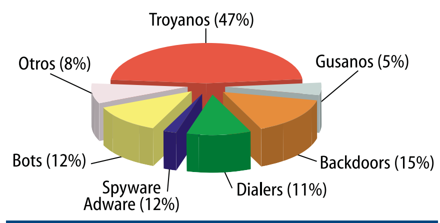
Un sitio web ruso ofrece un kit de software espía llamado WebAttaker por un costo de U$D 15.00.- ofreciendo además servicio de soporte técnico.

En promedio más de 300 muestras, entre gusanos, troyanos, spyware, phishing, pharming, adware, dialers, etc., llegan diariamente a Panda Labs, 100 de ellas serán catalogadas a lo largo del proceso

como malware. Luis Corrons nos comentaba “La percepción del público es que hay menos virus en circulación y es exactamente al revés: en el ultimo año y medio se ha detectado tanto malware como en los 14 años anteriores”. El proceso continúa en el área de Monitoring, que es quien prioriza y prepara estadísticas y reportes.
A partir de allí, los Especialistas en Malware, realizan lo que se llama procesos de Ingeniería Inversa y la Ejecución de archivos en ambientes cerrados, una de esas dos pantallas que posee cada especialista corresponde a una red cerrada en la cual

Hay troyanos preparados para interceptar y robar información de más de 240 bancos de todo el mundo, algunos locales

se conoce del primer al último bit, allí se “libera” el malware y se analizan cada uno de los cambios producidos a cualquier nivel. A su vez, cuando se requiere, cada especialista analiza el código assembler del malware, en forma minuciosa. Una vez que se determina que el archivo analizado es malware, se procede a generar los elementos de Detección de dicho malware, lo que comúnmente se denomina archivo de firmas, para ésto es necesario identificar una o varias cadenas hexadecimales únicas, mediante procesos automatizados



Distribución del Malware detectado en el primer cuatrimestre de 2006

se localizan e individualizan las mismas. Una vez desarrollada la “firma” esta debe ser testeada, no sólo a los efectos de que detecte realmente el malware, sino también que sea único, es decir que no haya ningún otro software o aplicativo que pueda ser confundido con éste. Conjuntamente con la detección se deben verificar y desarrollar las rutinas de Desinfección del Malware, sobre todo para el malware que se instala dentro de otros programas para camuflarse. Pasados todos los controles se actualiza la base de datos de firmas y se envía a Calidad para que proceda a chequear el nuevo archivo de firmas completo resultante, antes de colocarlo en Internet a disposición de los usuarios de todo el mundo.
El largo y complejo proceso que se debe repetir por cada uno de las más de 300 muestras diarias posee la mayor parte de sus pasos totalmente automatizados, con la utilización de software específico que también se desarrolla en el propio departamento y que se va ajustando a las necesidades y vaivenes de una dinámica del malware que ha cambiado totalmente en los últimos tiempos. Hoy en día no se busca infectar millones de equipos, sino que se realizan ataques dirigidos, se desarrollan troyanos con un fin muy específico y

La herramienta gratuita ActiveScan detecta en Argentina más de 2.000 malwares conocidos por mes que están instalados en los computadores de este país.

por lo general delictivo.
Quedan muchos temas por trasmitir, que fueron parte de la charla, por ejemplo, el cómo y porqué del nombre de los virus, las tentativas de estandarización, de nombres términos y criterios de clasificación, ejemplos como el COAST y el ASC, cuál es la peligrosa realidad de las redes de Bots, quienes y cómo las manejan, el problema del uso de técnicas de rootkits, nuevos vectores de ataques, el Phishing y las estafas bancarias detectadas y las aún no detectadas, la explotación de vulnerabilidades, cifras, estadísticas, casos, etc. ■

El Phishing, es una técnica de engaño que lleva al robo de cuentas bancarias y contraseñas. El último ataque detectado por PandaLabs ha sido dirigido a los clientes de la entidad bancaria SouthTrust. El mensaje de correo electrónico simula proceder de los responsables de seguridad de SouthTrust, afirmando que, debido a ciertas comprobaciones de seguridad, es preciso que el usuario acceda a una página web e introduzca sus datos confidenciales.
Como particularidad de este Phishing, se destaca que este ataque utiliza varios dominios de Internet para alojar las falsas páginas web, y que cada uno de ellos tiene asociadas varías direcciones IP con distintas localizaciones geográficas.



Además, y para mayor peligrosidad, el correo electrónico fraudulento hace uso de una función javascript que falsea la dirección que el usuario ve en la barra de su navegador, de manera que crea en todo momento que la página que está viendo se encuentra realmente en los servidores de SouthTrust, y que se trata de una conexión segura.

El 23 de Febrero de 2006, Panda Labs, recibe una muestra enviada por Truprevent desde Alemania, de un archivo que se llamaba 1284.tmp. Los expertos de Panda Labs decubren referencias a varios sitios web así como un servidor FTP. Éste era el comienzo de una trama de Venta de Troyanos a Medida!, el archivo detectado era sólo uno de los varios componentes que conformaban el troyano Briz A, y que era vendido personalizado con un precio básico de U$D 990.-, de allí la gama de precios y funcionalidades ascendían hasta una versión con garantía de no ser detectado por ningún software de seguridad.
Este troyano estaba compuesto por una DLL, que se instala como BHO (Browser Helper Object) sobre el IE y registra la información introducida al navegador.
Otro componente funciona como servidor web permitiendo conexión remota http. Un servidor FTP que envía la información capturada y por último una consola de administración.
La información obtenida por este troyano, contraseñas, de acceso a correos web, accesos a empresas de telecomunicaciones, líneas aéreas, servicios postales, sitios de apuestas, y una lista innumerable en esta nota, ocupaba 70,6 Mb, almacenada en más de 2000 archivos de texto, los usuarios comprometidos fueron 1.486, en 90 países.
Panda se contactó con RSA Security Ltd, trabajando en conjunto lograron luego de muchas acciones y contra-acciones que el sitio de venta de trojanos sea levantado definitivamente. Antes de eso en algunas de las páginas que caían y subían en determinado momento se pudo leer “Due to the pressure from China Bamboo Bear software, no more sales and development”



Cómo andamos con esto de la Seguridad



Ricardo D. Goldberger
Periodista Científico
Especialista en Informática y Nuevas Tecnologías. Produce el newsletter electrónico T-knos.

El 17 de mayo pasado se celebró por primera vez el Día Internacional de Internet y las Telecomunicaciones, sancionado en diciembre del año pasado durante la Cumbre de la Sociedad de la Información que se hizo en Túnez.

Acá en Argentina se festejó de distintas maneras el Día Mundial de Internet, con cursos online, seminarios, transmisiones en Red, etc. Y algunas empresas aprovecharon para publicar informes acerca del estado actual de distintas cosas. Así, por ejemplo, la firma comScore Networks propagó un estudio acerca de la cantidad de personas que navegan por Internet: "Unos 694 millones de personas de más de 15 años en todo el mundo están ahora navegando en Internet, lo cual representa cerca del 14% de la población total de ese grupo etario", según el cable de AP.

La buena noticia es que esta vez el estudio se tomó en todo el mundo, y los Estados Unidos ya no son la única "potencia" internetiana: "Hoy, los usuarios en Estados Unidos representan menos del 25% de los consumidores de Internet en el mundo, en comparación con los dos tercios de la audiencia global que representaban hace 10 años", dijo Peter Daboll, presidente de comScore Media Metrix.

Según el informe, Estados Unidos sigue manteniendo el primer lugar en el número de usuarios de Internet (152 millones), seguido por China (72 millones), Japón (52 millones), Alemania (32 millones) y Gran Bretaña (30 millones).

Bien, pero la idea no era hablar de este estudio en particular, sino de otro que liberó, el mismo 17 de mayo Symantec, llamado Informe sobre las Amenazas a la Seguridad en Internet. Cubre el periodo semestral que comprende del 1° de julio de 2005 al 31 de diciembre de 2005 e incluye un análisis de los ataques a la red, un estudio de las vulnerabilidades conocidas, y destaca los códigos maliciosos y otros riesgos de seguridad.

En su introducción, el reporte afirma: "Esta edición del Informe sobre las amenazas a la seguridad en Internet de Symantec marca un ***aumento destacable en las amenazas diseñadas para facilitar el delito en el ciberespacio***, actos delictivos que incorporan un componente informático o de Internet y un incremento en el uso del "crimeware" o software delictivo, es decir un programa que se usa para cometer actividades ilícitas en el ciberespacio.

Sigue diciendo el informe: "El nuevo panorama de las amenazas está dominado por amenazas como las redes bot, los códigos maliciosos modulares y los ataques dirigidos a las aplicaciones y navegadores Web. Aunque las tendencias anteriores se caracterizaban por ataques indiscriminados y ruidosos, como las amenazas combinadas y los gusanos, actualmente los ataques son silenciosos, difíciles de detectar y están dirigidos a un blanco específico. Los ataques tradicionales que fueron diseñados para destruir la información han dado paso a los ataques diseñados específicamente para robar información, generalmente por razones económicas."

Entre los resultados, sobresalen:

- Las amenazas de los códigos maliciosos que podían revelar información confidencial aumentaron, al pasar de 74% durante el último periodo del informe a 80%.
- Los códigos maliciosos modulares representaron el 88% de las muestras, frente al 77% en el periodo anterior.
- Incremento del 51% con respecto al anterior periodo de ataques diarios de negación de servicio (DoS).
- Un descenso del 11% en relación con el anterior periodo en computadoras infectadas con programas bot -una de las pocas variables positivas del informe- y
- China tuvo el segundo mayor incremento de computadoras infectadas, un aumento del 37%, que colocó a China en segundo lugar después de los Estados Unidos en esta categoría.

Éstos son algunos de los datos más importantes que hemos rescatado de este informe.

Me ha tocado recientemente discutir por radio, es decir, públicamente y al aire, la famosa hipótesis, nunca descartada del todo, que dice que los productores de malware son los mismos productores de software antimalware. No tengo ninguna evidencia que me permita confirmar o descartar esa hipótesis -si bien desde el sentido común, no me parece muy factible- pero cuando uno mira estas cifras, estos resultados, viniendo además de quien vienen, no puedo dejar de recordarla. ■

La Seguridad de las Aplicaciones y el Acceso

Desafíos y Soluciones

Para mejorar y proteger su información corporativa y aplicaciones, las empresas requieren de soluciones robustas y confiables, que les garanticen acceso seguro a todos los recursos necesarios.

Por **Christian Rovira**
Sr. Sales Engineer Southern Cone
Citrix Systems, Inc.

Dime qué problema tienes...

El aumento de la movilidad, la demanda de mayor flexibilidad laboral y el incremento de nuevos dispositivos, junto con los requerimientos específicos que estos fenómenos generan, exigen que los sistemas garanticen un acceso remoto seguro y confiable.

A fin de hacer frente a este fenómeno, Citrix propone su **Plataforma de Acceso Citrix Smart Access™**. Esta capacidad analiza cada escenario y entrega un nivel de acceso acorde, sin comprometer la seguridad, balanceando libertad del usuario y control de IT. En otras palabras, según quién sea el usuario y desde dónde se esté conectando, podrá ver las aplicaciones y documentos, pero no editarlos, editarlos pero no guardarlos localmente, o editar sin imprimir, entre otras opciones. De esta manera, provee seguridad en cualquier ambiente con tecnología sense-and-respond, mejora la productividad, a la vez que garantiza un ambiente de acceso totalmente seguro.

Por otra parte, si nos referimos a VPNs y la necesidad de eliminar los riesgos informáticos inherentes al acceso, Citrix Access Gateway™ se presenta como una solución sólida y confiable. Gracias a ésta, los usuarios remotos pueden conectarse a través de un cliente fácil de usar, con posibilidad de descargarlo de Internet, disfrutando de la experiencia de sentirse como si estuvieran frente a su escritorio de PC. En caso de que los usuarios cambien de ubicación o dispositivos, o pierdan conexión, el acceso "always-on" -o "siempre activo"- los reconecta automáticamente a sus documentos, sin interrumpir su trabajo. Además, para poder conectarse a la red de la compañía, el scanning de end-points asegura que los dispositivos de los usuarios permanezcan seguros.

> Citrix trabaja junto con socios estratégicos del prestigio mundial de Microsoft, IBM, HP, SAP y Dell, entre otros, para continuar desarrollando soluciones más potentes y robustas con estándares de próxima generación.

La última versión, Access Gateway 4.2, combina las mejores características de IPSec y SSL VPNs, con importantes resultados, entre los que se cuentan, por ejemplo, la instauración de un único punto de acceso seguro a cualquier aplicación o recurso de IT, tanto data como voz; bajo costo total de compra y mantenimiento; la mejor experiencia para el usuario y, además, refuerzo de la seguridad de la información.

Esta versión incorpora Advanced Access Control, una opción de software que incrementa el control sobre cómo la información es accedida, y extiende el acceso a más dispositivos y usuarios. Con esta solución, éste se convierte en un "dimmer switch", o regulador, donde el nivel de acceso puede ser configurado para cualquier escenario y sus características particulares.

El uso y administración de las claves constituye un asunto de gran preocupación dentro de las compañías. Para resolver esta situación, **Citrix Password Manager™** es la solución de Single Sign-On (SSO) más segura para acceder a Windows, a la Web, Host y a distintas aplicaciones. Citrix Password Manager se integra con todas las aplicaciones de manera simple y rápida, utilizando tecnología "no intrusiva" y sin necesidad de la creación de script o modificación de las aplicaciones para su correcto funcionamiento.

Su mecanismo consiste en que el usuario se



identifica sólo una vez con una única password y esta solución automatiza el logon, aplicación de políticas y cambio de contraseñas, haciendo de la conexión a las aplicaciones una experiencia más sencilla, rápida y segura. Adicionalmente, puede reducir los costos de Help Desk más de un 25%.

Ésta es la primera solución de **Single Sign-On** que permite a los usuarios resetear su password o abrir su cuenta de Windows desde su PC. En puestos de trabajo compartidos, común en hospitales, bancos, manufacturas y retails, Password Manager 4 presenta Hot Desktop para permitir a los usuarios realizar logon/off en segundos. Gracias a **Single Sign-On**, se elimina la carga de tener que recordar, entrar y cambiar periódicamente muchas contraseñas individuales, generalmente con diferentes requerimientos de caracteres, para poder acceder tanto a información como a aplicaciones.

Esta solución, además, se integra con otros productos, tales como HP Select Identity, Courion AccountCourier y IBM Tivoli Identity Manager, a fin de hacer **Single Sign-On** totalmente transparente para el usuario. Este nuevo lanzamiento también cuenta con identificación criptográfica para garantizar la integridad de la configuración y políticas para resguardarse contra vulnerabilidades y phishing.

En pocas palabras, Password Manager cambia, fundamentalmente, el típico acercamiento a la administración de múltiples contraseñas, trasladando esta importante responsabilidad a manos del departamento de IT.

Adicionalmente a crear una plataforma de Acceso Seguro se requiere proteger las aplicaciones Web sin degradar el rendimiento o el tiempo de respuesta de las mismas, **Citrix® NetScaler® Application Firewall** está especialmente diseñada para llevar la seguridad a otro nivel. Con este producto se detienen ataques que evaden firewalls de networks y dispositivos de IPS, además de proveer protección contra el robo de identidad asegurando información corporativa confidencial y data sensible de clientes. Esta solución, adicionalmente, cuenta con la tercera generación de **Adaptive Learning Engine** que puede, automáticamente, aprender el comportamiento de una aplicación y generar recomendaciones de políticas.

Citrix es la elección de 180.000 compañías para proveer acceso seguro, a usuarios locales y remotos, a aplicaciones cliente-servidor virtualizadas. Además permite al departamento de IT realizar un deployment y administración de las aplicaciones corporativas a la vez que proporciona un acceso seguro y on-demand a estos recursos, con el costo de propiedad (TCO) más bajo, la mayor seguridad y la mejor performance y escalabilidad.

La Seguridad desde el Diseño

La visión de Citrix como compañía sobre el acceso a través de **Citrix Access Platform** y su familia de productos, es posibilitar a las compañías entregar servicios de IT a cualquier usuario en cualquier lugar, sin comprometer la seguridad corporativa. Este modelo es conocido como "seguro por diseño", denominación impulsada por la propia empresa. A través de este esquema se le permite a las organizaciones, de cualquier tamaño, tratar la seguridad como una parte integral de su arquitectura.

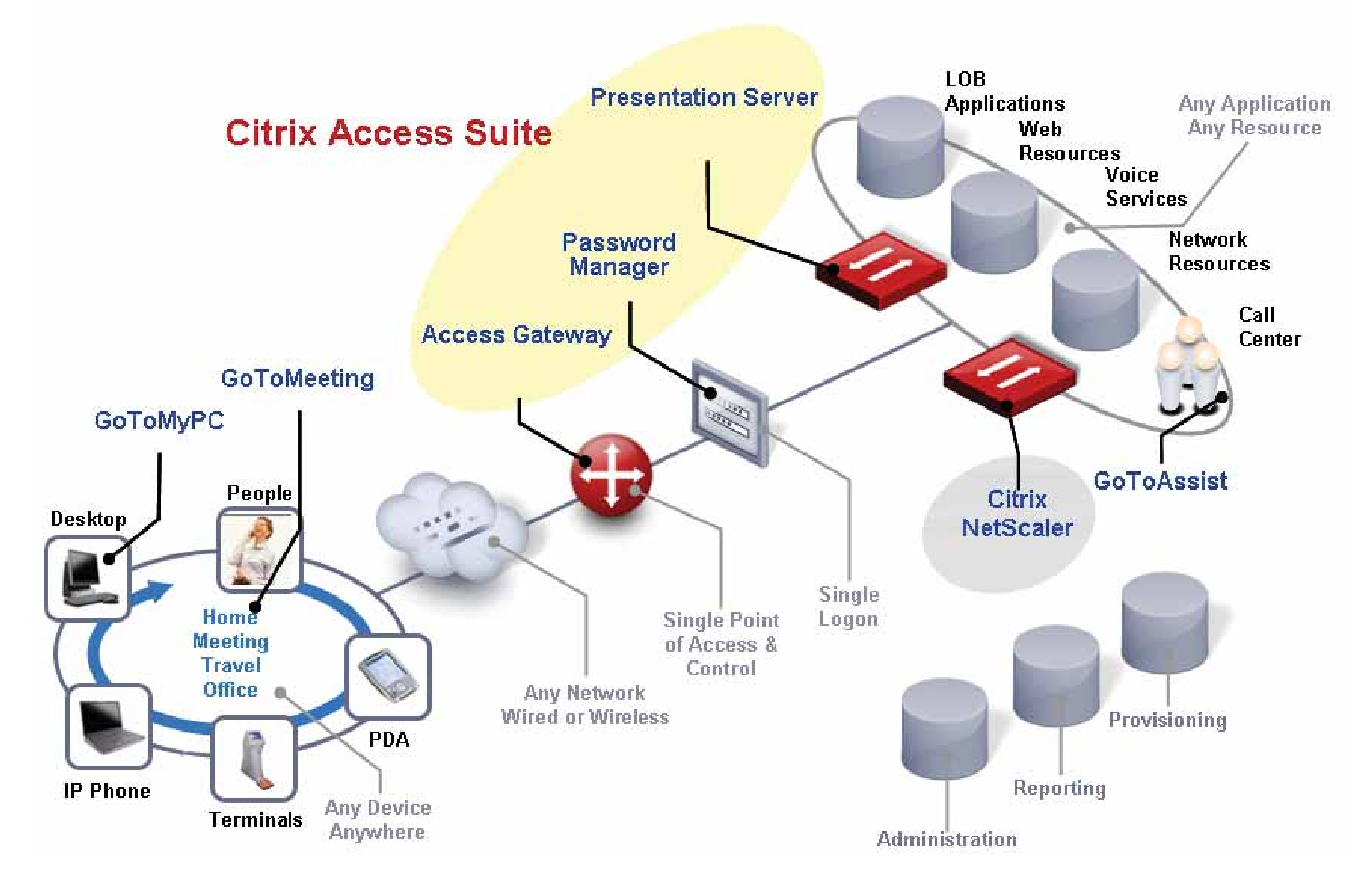
Para implementar una estrategia de acceso que contemple todos los aspectos necesarios para obtener una red segura, eficiente y un mejor desempeño de los negocios, es necesario tener en cuenta algunos conceptos íntimamente relacionados:

Virtualización de Aplicaciones: Con la virtualización de aplicaciones y la centralización de la información, los datos nunca salen fuera del centro de cómputos, permitiendo a los usuarios conectarse desde cualquier lugar, interna o externamente. La virtualización consigue esto extendiendo la seguridad de la red corporativa, evitando la instalación de las aplicaciones en dispositivos clientes, haciendo más sencillo proteger la información en los confines del data center.

Acceso Remoto Seguro: Permite a los empleados trabajar desde su hogar, garantizando acceso seguro a partners y consultores. Contar con recursos tercerizados y offshore puede ser dificultoso, o simplemente imposible, sin un acceso remoto seguro y confiable.

Control de Acceso: Los administradores pueden configurar políticas end-to-end para dictaminar controles según cada escenario. Estas políticas de acceso granular pueden tomar en cuenta usuarios, grupos, tipos de dispositivos, networks y seguridad de los end-points.

Administración de Autenticaciones: La Plataforma de Acceso protege, controla y refuerza la autenticación de usuarios para asegurar los recursos de las compañías.



Actualmente, más del 75% de los ataques de hackers apuntan a las vulnerabilidades de las aplicaciones. En esta coyuntura, la necesidad de implementar soluciones de Application Security se incrementa significativamente cada año.

Seguridad del End-point: En asociación con líderes de la industria, desde Microsoft a Symantec, la Plataforma de Acceso de Citrix optimiza innovadoras soluciones de end-point, centralizando la garantía de que sean seguros antes de permitir el acceso.

Exhaustivo Reporte y Auditoría: Los requisitos de auditoría implican acompañar el ciclo completo de la información, desde la interacción con end-points hasta con el data center. Para cumplir con estos requerimientos, los productos de Citrix soportan estos procesos para optimizar los negocios.

Acceso Instantáneo a las Aplicaciones Cliente Servidor a través de la Organización: **Citrix Presentation Server** hace más sencillo proveer acceso a los usuarios, incluyendo empleados locales y remotos, sucursales, partners y proveedores. Con su modelo centralizado, Presentation Server permite al departamento IT implementar y hacer un deploy de aplicaciones como CRM, SFA y ERP más rápidamente que si tuvieran que ser instaladas y configuradas en cada PC.

Consideraciones Finales sobre el Acceso y la Seguridad

En todas compañías, de cualquier mercado y tamaño, contar con soluciones sólidas y específicas es cada vez más imprescindible, tanto para mejorar y proteger las aplicaciones e información corporativa, como para potenciar los negocios de las organizaciones. Para Ésto, la Plataforma de Acceso de Citrix cuenta con importantes beneficios:

Mejor Performance: Citrix se destaca por la alta performance en la funcionalidad de las aplicaciones, incluso sobre conexiones Web y Wireless. Además, dado la poca demanda de ancho de banda de sus soulciones, su performance es similar a la de un software corriendo localmente.

Sólida Seguridad: Las soluciones de Citrix son "seguras por diseño", lo que significa que la seguridad está incorporada al desarrollo, no agregada posteriormente. Citrix Presentation Server refuerza la seguridad manteniendo las aplicaciones y data en el server detrás del firewall, en vez de exponerla en el desktop. La menor cantidad de data que viaja entre el servidor y el cliente es encriptada, y los administradores pueden controlar centralmente el acceso en el rol del usuario.

Acceso más Flexible: Presentation Server hace más sencillo para los empleados conectarse vía Web, desde su hogar u oficina temporal, a un server de backup y aplicaciones que necesiten para seguir generando ingresos.

Costo más bajo: Las poderosas herramientas de administración ayudan al departamento de IT a aumentar la eficiencia y reducir costos. Desde el data center, el staff de IT puede administrar aplicaciones, dar soporte y entrenar usuarios remotos, además de monitorear y reportar el sistema completo. En vez de utilizar tiempo y dinero viajando a distintos puntos, IT puede cumplir sus tareas desde la misma consola de Citrix.

El Distribuidor de Citrix para Cono Sur, Licencias OnLine, cuenta con una red de Partners Certificados para implementar proyectos de infraestructura de acceso en la región. Para mayor información, por favor comuníquese al 5166-5621 o escriba a *citrix@licenciasonline.com*. ■

Protección Anti-spyware

Por **Carlos Vaughn O´Connor**
Senior Security Editor
NEX IT Specialist

¿Existen empresas que utilizan métodos "non-santos" de modo de hacernos creer que "su" producto es el único capaz de detectar tal malware que supuestamente tiene nuestra máquina o peor aún que se dedican a implantar malware para luego darnos la solución?

Existen muchos productos anti-spyware, cada uno aduciendo poder detectar lo que otros no detectan. Muchas veces, al igual que en el caso de los virus nos preguntamos si no habrá un negocio de ciertas empresas engañando sobre la existencia de los mismos o peor aún introduciendo malware en nuestras máquinas para luego invitarnos a usar su herramienta mágica.

Ésto es exactamente lo que plantea y corrobora Mark Russinovich en su blog http://www.sysinternals.com/Blog/: "La conspiración Antispyware"

Mark nos dice que uno de los modos más comunes de engañar es cuando ciertas publicidades nos presentan banners o pop-ups que parecen errores de Windows y nos indican tomar una acción inmediata. En cualquier lugar que toquemos de ese banner no lleva a un link como el de www.myspwarecleaner.com. La página que nos presenta es como mensaje de error del IE (Internet Explorer) e induce al navegador a bajarse e instalar "su" anti-spyware [Fig.1 y 2].

Mark bajó y probó la herramienta sobre una máquina con Windows XP recién instalado y sin posibilidad de contaminación. El spyware detectó una docena de infecciones "extreme risk" y "high risk" que incluían varios cookies inofensivos dejados por MSN.com y varios COM del sistema operativo. Todos los identificó como spyware [Fig.3].

Por supuesto para removerlos el usuario debería pagar una registración. ¿Quién hace Spyware Cleaner? No aparece en la web-page pero corriendo el Whois Mark finalmente encontró su dueño: Gary Preston de Secure Computer LLC!!!!!.

Éste no es un caso aislado y aún más, desafortunadamente hay quienes infectan máquinas para luego a través de un chantaje logran que se les compre el anti-spyware.

Mark nos narra el caso "Spyaxe" una de las infecciones que más se discuten en los foros de Sysinternals. El malware continuamente muestra pop-ups (como en la figura 4) diciendo a los usuarios que Windows ha detectado que sus máquinas están infectadas. Clickeando uno de estos aparece la web-page de www.spyaxe.com. La empresa dueña del dominio por supuesto niega relación alguna con estos incidentes!!!!

Nuevamente, este es un caso entre muchos.

Invitamos a conocer el blog de Mark donde incluso aparece una película con un ejemplo sobre todo ésto, para el caso de SpySheriff otro ladronzuelo del antispyware. NO deje de estudiarla.

Mark concluye su nota, indicando que ya algunos fiscales están actuando sobre estos casos y menciona que estos casos lamentablemente generan dudas sobre toda la industria.

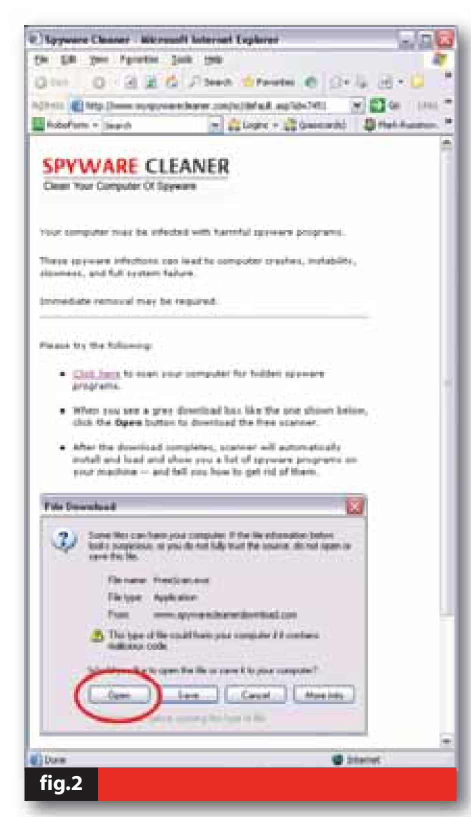


fig.2

Warning - Spyware Notice
Your computer may be infected with harmful spyware programs. Immediate removal may be required. To scan, click "Yes" below.
Yes No
advertisement

fig.1



fig.3



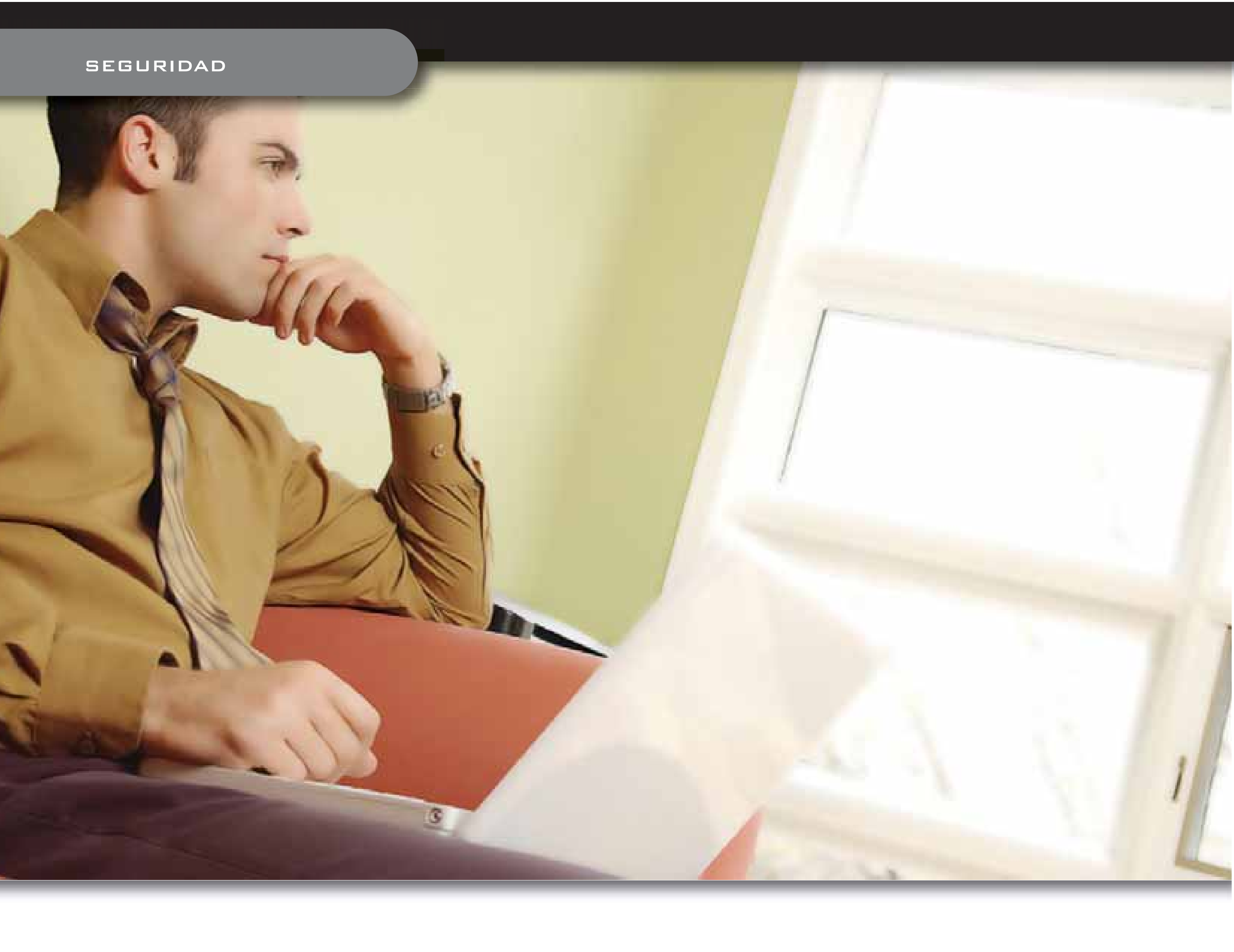
fig.4

Acerca de Mark Russinovich



Mark Russinovich es ingeniero en software y escritor. Escribe en forma regular en la prestigiosa revista "Windows IT Pro" fundamentalmente sobre la arquitectura de Windows. Es autor de muchas herramientas populares usadas desde Windows NT hasta 2003 Server. Es un experto en Windows y un MVP de Microsoft.

Mucho de su trabajo lo realizó con David Solomon y puede apreciarse en su webpage http://www.sysinternals.com/ dotada de innumerables herramientas freeware muy útiles. La parte comercial de su trabajo la realiza en Winternals Software.



P

Permítanme que comencemos con esta frase trillada pero no por eso menos cierta, sobre todo cuando hablamos de un profesional de Seguridad de la Información.

En general, quienes trabajamos en IT no solemos ser la más comunicativa del mundo. Desde un principio aprendimos que en nuestra industria el conocimiento es poder, y cuanto menos tengan los demás, mejor es para nosotros.

Quizá los primeros que lograron superar este paradigma fueron los desarrolladores. A medida que los proyectos crecieron, tuvieron que aprender a convivir entre sí, trabajar en grupos y con el tiempo, descubrieron que colaborando se podía llegar más lejos y más rápido.

Compartiendo ideas, problemas, soluciones, y finalmente código y componentes, llegaron a evolucionar en una verdadera comunidad. Así, no creo que exista mucha duda que hoy en día, no hay otra área de IT que haya desarrollado una conciencia de la importancia de la comunidad como ésta.

Probablemente el polo opuesto sea ocupado por la gente de seguridad de la información. En parte por naturaleza -por algo se termina trabajando en ésto-, en parte porque nuestras tareas nos enseñan a ser reservados, la realidad es que la gente de seguridad está sola. Y estar solos en esta posición nos hace vulnerables. Ya lo dejo claro el Martín Fierro, con eso que "Los hermanos sean unidos, / Porque esa es la ley primera; / Tengan unión verdadera / En cualquier tiempo que sea, / Porque si entre ellos pelean / Los devoran los de ajuera.". Nunca la metáfora fue más precisa que en nuestro caso.

La matemática no está de nuestro lado. La cantidad de recursos, tanto económicos como de tiempo que dispone el área de seguridad son, siendo generoso, muy limitados. Si medimos estos recursos contra los que tienen el universo de adversarios potenciales, es fácil darse cuenta que estamos en desventaja.

Para complicar aún más el problema, tenemos la asimetría básica de la seguridad: el (o los) encargado de seguridad tiene como misión cubrir todos los problemas potenciales de seguridad existentes y los que aparecen cada día, mientras que cualquiera de nuestros atacantes -internos y externos-, sólo necesitan encontrar una única vulnerabilidad para hacer destrozos.

Tanto por una cuestión de imagen de nuestras compañías, como por no exponernos aún más, entre tantas otras razones, optamos por hacer mutis por el foro respecto de los inconvenientes sufridos.

Flaco favor nos hacemos. Que nosotros dejemos de reportar problemas, no evita que el underground se entere inmediatamente, pero sí que otros puedan protegerse a tiempo, que se puedan generar métricas -punto fundamental para tomar decisiones informadas y no usando el famoso método de los cinco dígitos oscilantes-, adoptar medidas legales, recibir ayuda de quienes ya padecieron lo mismo y otras tantas cosas. Por supuesto, no es cuestión de andar ventilando a los cuatro vientos nuestras debilidades, pero si hay algo que se esta haciendo cada vez más patente, es la necesidad de puntos de contacto con otros miembros del sector, que comparten nuestra problemática y con los que podemos relacionarnos y enriquecernos mutuamente.

No importa si es un tema de seguridad de red, de desarrollo, de actualización de parches, de concientización de usuarios o de seguridad física de los archivos. Si tiene información -y qué no tiene información hoy en día- es de nuestra incumbencia.

Y, por si todas estas incumbencias no bastaran, el rol de seguridad ya no es uno solamente técnico, sino que se ha expandido para abarcar desde aspectos de management -la seguridad como soporte y en función del negocio, no al revés- y de capacitación de personal hasta aspectos legales, edilicios y de seguridad física. ¿No lo creen? Piensen en un centro de cómputos debajo de un baño, en

No es bueno que el hombre esté solo.

Una mirada rápida sobre la problemática que determina la necesidad de una verdadera comunidad de seguridad de la información, y un breve resumen de las iniciativas disponibles en la actualidad, en las cuales participar.

Por Lic. **Nicolás Mautner**
Licenciado en Sistemas
CISSP Certified

una planta baja vidriada o en un subsuelo.
Ésto nos lleva a otro problema que podemos ver frecuentemente. En la mayor parte de las áreas de la industria, los roles y funciones que cumplen los profesionales son claros. A nadie se le ocurriría pedirle a un Administrador de Red que desarrolle una aplicación contable, ni a un programador VB que configure un servidor de mail en Linux.
En Seguridad de la Información ésto no sucede. Las búsquedas de personal de InfoSec son, en el mejor de los casos, confusas. No es una práctica habitual relevar para los recursos de seguridad las tareas de cada rol, los roles que pueden cumplirse en cada puesto y en armar una matriz de incompatibilidades relacionada, de forma tal de no buscar a "alguien de seguridad", sino a un profesional con experiencia en el perfil deseado.
Finalmente, creo que uno de los aspectos más complejos relacionados con el área es la capacitación.
La oferta a nivel terciario, de grado y postgrado, además de francamente escasa, es poco conocida - ¿Cómo esperamos tener gente capacitada si en la mayor parte de las carreras relacionadas las materias de seguridad de la información no existen o, en el mejor de los casos, son optativas? -. Justamente por esta falta de opciones de capacitación (y por lo tanto de formas más o menos estándares y creíbles de acreditación de conocimientos), toman aún más importancia las certificaciones profesionales.
Cada vez son más las empresas que consideran estas certificaciones un plus importante a la hora de seleccionar su personal, aunque su variedad (desde lo completamente generalista hasta lo absolutamente específico, y desde lo independiente hasta las certificaciones de empresas proveedoras-caso CISCO, Symantec y muchas otras-), unido a una falta de conocimiento cabal de los alcances de cada una, hace que no siempre elijamos la que más se adapte a nuestra experiencia o necesidades.
Es aconsejable, antes de elegir una certificación (que suelen ser bastante caros e insumir una nada despreciable cantidad de tiempo y esfuerzo) tomarse un tiempo para evaluar cuales hay en el mercado, que tan reputadas y buscadas son en el mercado al que apuntemos (local, regional, o internacional) y que costo/beneficio traería a nuestro desarrollo profesional. Si bien un análisis de la oferta en materia de certificaciones de seguridad excede ampliamente el objeto del presente artículo, existen en la Web numerosas fuentes de información al respecto. A quien le interese, un buen punto de inicio es www.issa.org/certifications.html
Para responder a estas situaciones, lentamente en el país y en la región se están dando los primeros pasos, por medio de diferentes tipos de iniciativas, las cuales, cada cual a su modo, intentan crear espacios válidos y necesarios para que los profesionales de Seguridad de la Información puedan conectarse y convertirse de un grupo de gente que trabaja en lo mismo, a una comunidad de profesionales y practicantes integrada y participativa.
Sin ánimos de hacer listas exhaustivas, sino de comentar sobre lo que conozco, son dignas de mencionar:

ADACSI
Es la Asociación de Auditoría y Control de Sistemas de la Información. Es el capítulo local de la internacional ISACA, y está integrado principalmente por auditores de sistemas. Internacionalmente, fue creada en 1976 y cuentan con más de 50.000 miembros. Tienen una intensa actividad académica en forma de cursos a lo largo de todo el año.

ASIS International
Es una asociación internacional de profesionales de seguridad. Está formada por profesionales con al menos una década de experiencia en dirección de seguridad y dicta anualmente el curso de pre-

paración para la prestigiosa certificación CPP. Originada en 1955, tienen globalmente más de 33.000 miembros, y se enfoca en la dirección de seguridad como un todo, incluyendo profesionales de todas las ramas, como ser personal de agencias de seguridad, abogados y arquitectos entre otros.
ASIAR es una asociación creada en 2005 por profesionales que trabajan en el área de seguridad de la información, el ingreso a ASIAR es por postulación con CV y su posterior escrutinio por parte de un comité.

CASI (Consejo Argentino de Seguridad de la Información)

Es una iniciativa que organizó Microsoft hacia fines del 2004, con el fin de generar un espacio de discusión entre los responsables de seguridad de empresas de gran envergadura, en diferentes industrias. Es de destacar que Microsoft no es "dueño" de este consejo ni participa como miembro del mismo, sino que es su impulsor y brinda las facilidades para su continuidad de operación.

Acerca del Lic. Nicolás Mautner

Nicolás Mautner es Licenciado en Sistemas egresado de la Universidad CAECE, y se ha certificado como CISSP.
Se ha desarrollado profesionalmente en varias áreas diferentes de Tecnología y Sistemas, como ser análisis y desarrollo de aplicaciones, dirección de proyectos, evaluación de tecnologías, y otros.
En los últimos años ha trabajado como Auditor de Sistemas y Consultor en Seguridad de la Información.
Es fundador y actual presidente del capítulo argentino de ISSA, miembro del Consejo Argentino de Seguridad de la Información y del comité académico de SEGURINFO desde su creación.
Es profesor en la Universidad CAECE de Seguridad Informática, Taller de Seguridad Informática I y II, y Seminario de Seguridad Informática.
Ha dado conferencias en congresos y publicado artículos relacionados con la materia.

Además, el CASI genera, a lo largo del año, papers y material respecto a temas claves que afectan a los diferentes aspectos del gerenciamiento de InfoSec. El ingreso al CASI se realiza por votación de los miembros.

SEGURINFO

Creada en 2004, es nada menos que el grupo de seguridad de la ya antológica USUARIA. Desde su fundación, con un importante énfasis en su comité académico, SEGURINFO organiza anualmente el congreso de seguridad homónimo.

ISSA Argentina

Establecida en 2004, es el capítulo local de ISSA (Information Systems Security Association) y está formada por profesionales y practicantes de la seguridad de la información. Busca promover el uso de buenas prácticas que aseguren la confidencialidad, integridad y disponibilidad de la información. Mundialmente, cuenta con más de 13.000 miembros formando 110 capítulos locales en 24 países.
La inscripción es abierta y realiza diversas actividades, desde grupos de investigación (awareness, métricas, etc.) hasta actividades de capacitación tanto a nivel técnico como aspectos de gerenciamiento de la seguridad de la información. Sus objetivos son mantenerse como un referente independiente -no alineado a ningún interés comercial- y agnóstico a cualquier producto, tecnología o servicio, y colaborar con el desarrollo profesional de sus miembros. Bajo esta misma línea de independencia, ISSA no auspicia ninguna certificación profesional en particular.

¿En cuál participar?

En el fondo, la organización a la cual cada uno decide favorecer con su participación -tengamos ésto siempre en mente, una organización no nos hace el favor de dejarnos participar, nosotros le hacemos el favor de dedicarle nuestro tiempo y capacidades- debería depender de la medida en que coincidan los objetivos personales con los de la entidad elegida. Dicen que el tiempo es tirano, y la idea de repartir el poco que nos queda después de hacer nuestro trabajo entre diversas organizaciones es, en el mejor de los casos, poco estimulante. Es mucho más significativo, para el individuo y para la comunidad -al menos inicialmente-, elegir un grupo y trabajar en él a conciencia, que pertenecer a varios, ser oyente en todos y no aportar a ninguno.
Como es de esperar, cada vez más, casi todos estos grupos interactúan entre sí, tratando de complementar sus capacidades y habilidades, y así evitar duplicar esfuerzos. Aunque cada uno tenga una visión un poco más orientada a uno u otro tema en particular, sus objetivos son comunes y la comunidad de seguridad es una sola y no tan extensa. La práctica viene demostrando hace tiempo que cuando un grupo intenta sesgarse de los demás, más que una posición de elitismo consigue una de ostracismo.
No importa donde elijamos pertenecer, es fundamental recordar que la participación de los miembros es lo único que puede hacer subsistir a cualquier grupo de profesionales. No esperemos de la comunidad nada que no estemos dispuestos a darle. Si no queremos invertir nuestro trabajo en ella, o tememos someternos a la evaluación de los demás -el problema con hacer es que todo lo que hacemos es siempre susceptible a la crítica y al escarnio-, no deberíamos pedirle que genere contenidos de valor a nuestra profesión.
A fin de cuentas, una asociación es útil en la medida en que sus miembros se beneficien de participar en ella, tanto por su aporte como por el de sus pares.
Dicho ésto, los invito a sumarse a una comunidad, a colaborar, descubrir las ventajas de ser parte de ella y ver como en seguridad como en tantos otros aspectos, no es bueno que el hombre este solo. ■

Para más información:
ISSA: *www.issa.org*
ISSA Argentina: *www.issaarba.org*
ASIS: *www.asisonline.org*
ADACSI: *www.adacsi.org.ar*
SEGURINFO: *www.segurinfo.org.ar*
CASI: *casi@casi-ba.com.ar*
ASIAR: *info@asiar.org.ar*



TippingPoint
a division of 3Com

NEX IT entrevistó a expertos locales de 3COM buscando conocer más sobre TippingPoint y su relación con las PYMEs y el mercado corporativo.

NEX: ¿Qué beneficios obtuvo 3Com con la compra de TippingPoint y cuándo se realiza?
R: La adquisición de TippingPoint se realiza en Febrero del año 2005, luego de un amplio estudio y búsqueda de empresas con un reconocido desempeño en el mercado de Seguridad Informática, y principalmente que dispongan de una solución diferencial como es un IPS (Sistema de Prevención de Intrusos).
Esta importante compra significó para 3Com la apertura y llegada a nuevos mercados, nuevas oportunidades de hacer negocios, como también ha generado despertar el interés de los encargados de seguridad de muchas de las más grandes empresas de la región.

NEX: ¿Qué nuevas soluciones técnicas propone esta adquisición?
R: Principalmente TippingPoint propone un appliance Sistema de Prevención de Intrusos (IPS) de gran performance basados en ASICs.

NEX: ¿Cuál es la historia de TippingPoint y su expertise en Intrusion Prevention?
R: TippingPoint nació directamente con el desarrollo propio de un IPS en el año 2001. A partir de allí tuvo en sostenido crecimiento a nivel de revenue y market share en el mercado Americano (USA/Canadá) y Europeo.
A partir de la adquisición, el market share sigue creciendo y conquistando mercados a los que antes no podíamos llegar con ciertas soluciones.
Hoy no sólo tenemos la mejor solución de seguridad sino también un completo portfolio de productos de excelente performance y precios más que atractivos. En 3Com seguimos pensando en soluciones que se adapten a las necesidades del cliente y no al revés.

NEX: ¿Dónde están ubicados sus laboratorios de investigación?
R: El laboratorio de investigación conocido como "Threat Management Center" está ubicado en Austin, Texas.

NEX: ¿Qué ofrecen las soluciones de TippingPoint?
R: Se disponen de soluciones de appliance IPS con los modelos TP50, TP200, TP400, TP1200, TP2400 y TP5000E; en donde el número hace referencia al throughput total en megabits soportado por cada equipo y se presentan con interfaces de cobre y fibra o combinación de ambas, hasta un máximo de 8 puertos (4 segmentos físicos).
Adicionalmente a estas soluciones se incorporaron este año equipos como el TippingPoint X505, que sobre la plataforma del IPS más chico, se suma principalmente las funcionalidades de Firewall, Concentrador VPN y Filtrado de Contenido Web, entre otras.
También se suma otro lanzamiento como el TP M60, un IPS de 60Gb throughput del tipo chasis de gran escalabilidad para el segmento Carrier Class.

TippingPoint es símbolo de IPS (Intrusion Prevention System/Sistema de Prevencion de Intrusos).
3Com es conocido por sus productos para infraestructura de redes. La compañía fue co-fundada en 1979 por Rober Metcalfe y tiene su central en Marlborough, Massachusetts. Su nombre proviene del foco principal de la empresa: "Computers, Communication and Compatibility".
Robert Metcalfe inventó Ethernet en Xerox PARC y subsecuentemente co-fundó 3Com en 1979. 3Com comenzó fabricando tarjetas Ethernet para la PCs IBM y un conjunto de software y equipos orientados a las PCs de modo de poder compartir servicios sobre LANs usando el protocolo XNS.
En enero de 2005, 3COM adquiere TippingPoint (www.tippingpoint.com) la prestigiosa firma especializada en IPS (Intrusion Prevention System).

NEX: ¿A qué mercado están dirigidas sus soluciones?
R: Se ofrecen soluciones tanto para las PyMEs como para las empresas de perfil Corporativo y Carriers. Esta característica diferencial la tenemos dado el amplio abanico de equipos con el que contamos.

NEX: ¿Es posible ampliar más sobre las siguientes características de las soluciones: Seguridad sobre VoIP, Administración del bandwidth, Protección Peer to Peer, Posibilidad de bloquear codigo malicioso casi sin ningun tuning especial?

R: • Seguridad sobre VoIP
La tecnología IPS de TippingPoint protege a las redes contra los conocidos cyber-ataques o amenazas de hoy, así como futuras vulnerabilidades específicas de VoIP y amenazas que están comenzando a ser emergentes.
Las implementaciones de VoIP enfrentan una variedad de amenazas desde las diferentes capas de networking, así como desde diferentes áreas de confianza dentro de la red. Un atacante podría comprometer un gateway VoIP, causar un ataque de Denegación de Servicio al sistema central (Call Manager), explotar una vulnerabilidad en una implementación sobre el protocolo SIP o tratar de

escuchar llamadas a través de un TCP Hijacking, UDP spoofing o manipulación de una aplicación.
La disponibilidad de los servicios VoIP dependen directamente de la disponibilidad de la infraestructura IP donde éstos corren. Cualquier ataque DDoS como ser SYN Floods o similar, que comprometa los recursos de la red podría impactar severamente en todas la comunicaciones VoIP. También gusanos o hosts zombies escaneando servers vulnerables pueden causar tráfico no intencional disminuyendo la disponibilidad de los servicios VoIP.
A nivel de aplicación VoIP existen distintos ataques que pueden interrumpir o manipular un servicio:
Denial of Service: spoofeando su identidad, un atacante puede causar un denial-of-service en una red VoIP basado en SIP, enviando un mensaje "Cancel" o "Bye" a un integrante y terminar la llamada. Como SIP está basado en UDP, mandar un paquete spoof ICMP con el mensaje "port unreachable" a una llamada establecida puede resultar un DoS.
Eavesdropping: un atacante con acceso local a la red VoIP puede esnifear (olfatear) el tráfico de red y descifrar una conversación de voz. Una herramienta llamada VOMIT (Voice Over Misconfigured Internet Telephones) puede ser bajada para fácilmente realizar ese ataque.
Call Hijacking: un intruso puede spoofear una respuesta SIP, indicando al otro integrante que la llamada ha sido movida a una dirección SIP "nueva", y "secuestrar" la llamada.
Mas allá de un firewall en cualquier infraestructura IT de hoy, la tecnología de Prevención de Intrusión se volverá un componente requerido en cualquier implementación VoIP. El IPS de TippingPoint ofrece una única, total seguridad y alta performance para proteger los desarrollos VoIP. TippingPoint previene de inundaciones DDoS, virus, gusanos, buffer overflows, y muchos otros ataques maliciosos contra la infraestructura IP y los servicios VoIP

• Administration del bandwidth
Mediante la plataforma TippingPoint se permite proteger y garantizar ancho de banda para aquellas aplicaciones críticas de cualquier empresa; aplicando reglas como "rate limit".

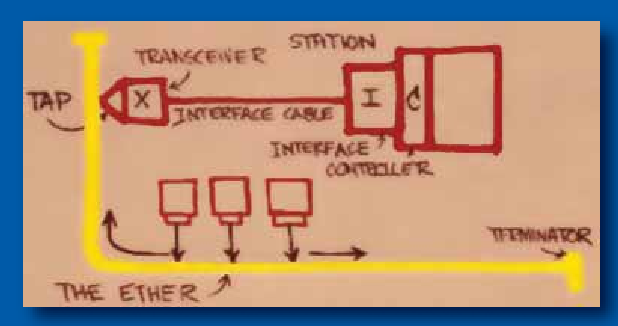
• Protección Peer-to-Peer
TippingPoint ofrece protección ante cualquier tráfico maligno que ingrese utilizando servicios P2P; así como también protege los recursos y disponibilidad de la red por el mal uso de herramientas P2P.

• Posibilidad de bloquear código malicioso con casi ningún tuning especial
Ésto es posible por que toda la línea de productos ofrece el denominado "Recomended Settings", por el cual el equipo viene pre-configurado de fábrica con filtros/firmas ya habilitados sobre las amenazas más críticas conocidas hasta el momento tanto a nivel aplicativo como de infraestructura; garantizando un mínimo tuning.

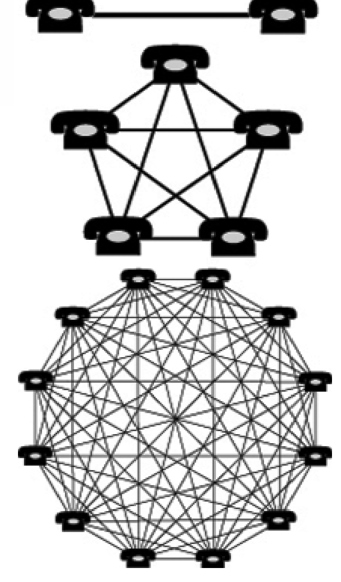
Quién es Robert Metcalfe



Robert "Bob" Metcalfe nació en Brooklyn, Nueva York, en 1947. Desde pequeño tuvo un ávido interés por la tecnología, que de grande lo llevó a desarrollar el estándar de red más popular del mundo, Ethernet. También fundó la empresa 3Com y formuló la Ley de Metcalfe.
Metcalfe hizo sus estudios de grado en el MIT, donde se graduó en 1969 con los títulos de Bachiller en Ingeniería Eléctrica y de Administración de Negocios (este último por la Sloan School of Management del MIT). Sólo un año después, obtuvo la maestría en Matemáticas Aplicadas en la prestigiosa Universidad de Harvard, para terminar sus estudios en 1973 doctorándose en Ciencias de la Computación con una tesis sobre conmutación de paquetes escrita mientras trabajaba en el Proyecto MAC del MIT.
Mientras finalizaba su doctorado en 1972 Metcalfe comenzó a trabajar para Xerox en el centro de desarrollo de Palo Alto (Xerox PARC), donde conoció a D. R. Boggs. Metcalfe y Boggs inventaron lo que llegó a conocerse como Ethernet, la tecnología de área local que hoy se utiliza para conectar a millones de computadoras en todo el mundo.
En 1979, Metcalfe abandonó Xerox para fundar 3Com en Santa Clara (California).
Desde 3Com, Metcalfe trabajó para promover la conectividad entre PCs utilizando la tecnología Ethernet. A pesar de no lograr la participación de IBM, Metcalfe logró el apoyo de DEC, Xerox e Intel, y logró imponer Ethernet como el estándar más popular en conectividad de redes LAN.
En 1980 recibió el Premio Grace Murray Hopper de la Association for Computing Machinery por su trabajo en el desarrollo de redes locales, específicamente Ethernet.
En 1990 abandonó 3Com tras una disputa con la junta directiva. En ese tiempo logró que su empresa se convirtiese en una de las empresas que aparecen en la lista de Fortune 500 y un referente en el área de conectividad. A día de hoy, Metcalfe sigue presente en el mercado informático, tanto con sus ensayos como con sus charlas. Gracias Robert Metcalfe. ¿Dónde estaríamos sin la invención de Ethernet? *(Fuente Wikipedia)*



La ley de Metcalfe



La ley de Metcalfe dice que el valor de un sistema de comunicaciones aumenta proporcionalmente al cuadrado del número de usuarios del sistema (N^2). Para ser más exactos y puesto que un usuario no se puede conectar consigo mismo, la fórmula real es:

$$\frac{n(n-1)}{2}$$

Formulada por primera vez por Robert Metcalfe en relación a Ethernet, la ley de Metcalfe explica muchos de los efectos de red de las tecnologías y redes de comunicación, como Internet o la World Wide Web. La ley suele ilustrarse con el ejemplo de aparatos de fax: un único aparato de fax es inútil, pero el valor de cada aparato de fax aumenta con el número total de faxes en la red puesto que el número total de personas que pueden enviar y recibir documentos crece. Ésto contrasta con los modelos tradicionales de la Ley de la oferta y la demanda, donde si aumenta la cantidad de algo su valor disminuye. *(Fuente Wikipedia)*

Nota 4



SEGURIDAD en LINUX

Por **Luis H. Otegui**

Tal y como dice el refrán, el ojo del dueño engorda al ganado. Es así que nos enfrentamos a esta cuarta nota de la serie, la cual tratará acerca de cómo mantenernos al día con actualizaciones, y relevar periódicamente el estado de nuestra red sin que esto suponga un suplicio.

Las prácticas sistemáticas de seguridad son las más difíciles de mantener, dado que exigen algo más que conocimientos. Nos exigen constancia, compromiso, y mantener la mente abierta a nuevas ideas. Normalmente, al encontrar una solución que nos permita hacer las cosas de manera más fácil, la adoptaremos de inmediato. Pero si no sabemos que existe esa solución, difícilmente podamos probarla…

En esta cuarta nota, haremos un repaso por las tecnologías y soluciones disponibles a la hora de realizar monitoreos sistemáticos del estado de la red.

De 0 a 100 en 5 Notas



Panorama general

Cuando hablamos de herramientas para sistematizar las prácticas de seguridad, necesariamente debemos estandarizar la mayor cantidad de procedimientos posibles. Las razones son varias. En primer lugar, la sistematización nos permitirá realizar estas tareas de modo más eficiente -tanto más cuanto más grande sea la red a monitorear. Segundo, evitará que "pequemos por omisión", dejando de lado algún chequeo en la vorágine de pruebas a realizar. Y tercero, nos permitirá uniformar la salida de los distintos procesos y, si tenemos suerte, unificar la misma en alguna forma de informe. De esta manera, podremos cumplir con la segunda parte de una auditoría de seguridad de manera mucho más eficiente.

¿Cuál es la segunda parte? Aquella que involucra tomar alguna medida respecto a las anomalías y/o fallos desvelados por nuestra auditoría. Pero primero, establezcamos un orden de prioridades.

La lista del súper

Como a la hora de hacer compras, deberemos, antes de salir, relevar qué tenemos en casa, y qué nos hará falta incorporar. Luego, de la oferta existente, podremos elegir con qué producto cubriremos el faltante de nuestra despensa…

Siempre pensando el monitoreo y el control desde hosts corriendo sistemas Linux, una lista básica de software necesario para comenzar a controlar de manera seria le desempeño de los servidores y la red incluye:

- *Un monitor de intrusiones basado en host (HIDS).*
- *Un monitor de intrusiones basado en red (NIDS).*
- *Un monitor de tráfico.*
- *Un monitor de estado de la red.*
- *Un analizador de vulnerabilidades.*
- *Un sistema de alertas (vía web, sms, etc.).*
- *Un analizador de logs, o un servidor de logs.*
- *Una suscripción a un buen servicio de alertas, o CERT.*

OK, terminada nuestra primera check-list, podemos ver qué oferta tenemos para cada ítem en el mercado de software libre:

- Monitores de intrusiones basados en hosts:

Acá las opciones más conocidas para tener un HIDS básico que trabaje de manera activa son Portsentry (1), un detector de port scannings, o Snort (2), aunque en mi opinión, a éste último, ésta categoría le queda chica. Como HIDS pasivos podemos mencionar a Tripwire (3) o AIDE (4). Los llamamos pasivos porque sólo pueden avisarnos de una intrusión después de que ésta ocurrió (en la jerga también se los llama FIDS, o Filesystem-based Intrusión Detection Systems). Los HIDS activos nos avisan de un intento de intrusión mientras éste ocurre. Tripwire y AIDE sólo se dan cuenta de cambios en el sistema de archivos, al igual que Chkrootkit (5). Otra opción menos conocida, pero igualmente válida, y que les recomiendo mirar, es OSSEC (6).

Lo ideal, sería colocar un NIDS en cada host de la DMZ, aunque con un FIDS que realice corridas periódicamente y nos informe sus resultados debería bastar.

- Monitores de intrusiones basados en red:

El estándar de facto en ésta categoría es Snort. Bien configurado, nos puede avisar a su frontend web de los intentos de intrusión, port scannings, y actividades anómalas varias, como ataques DDoS y de otros estilos. Un hermanito menor de Snort es Bro (7) (¡¡Perdón por el juego de palabras!!). Aún no es -según sus autores- tan potente y confiable como Snort. Sus resultados pueden ser interpretados y ¿Mejor? visualizados con la ayuda del frontend web The Spinning Cube (8), desarrollado ex profeso para la conferencia SC-03. Una tercera opción, que en primera aproximación luce interesante, es My Net Watchman (9). Lo diferente de MNW es cómo trabaja. Nosotros instalamos un agente sobre nuestro sistema, y el mismo analiza la salida de los logs del firewall, y comunica los incidentes a un servidor central. Luego, dependiendo de la severidad del ataque, nos informa vía correo del incidente. La idea central detrás de éste producto es poder tomar conciencia lo antes posible de un problema a gran escala, no de ataques aislados a un host o red en particular.

Lo ideal sería destinar una máquina a monitorear



El ojo del Dueño...

la red mediante Snort, y colocar la misma como un gateway entre la línea de firewalls externos y el interior de nuestra red.

- Monitores de tráfico:

Acá la cosa es qué nos interesa monitorear, y qué nivel de invasión de la privacidad de nuestros usuarios queremos vulnerar. Un muy potente analizador de tráfico de red en tiempo casi real es Ntop (10). El mismo es capaz de individualizar el tráfico de cada host, discriminarlo por tipo (mail, http, https, programas p2p, etc.), y presentarlo vía un frontend web que ya trae integrado. Nos informa además y si queremos de los puertos y direcciones de destino de cada conexión, aunque esto puede resultar bastante pesado para el host donde lo corramos. Una opción más liviana es IPAudit (11), integrándolo con su frontend web IPaudit-web (12). El mismo corre como un script que es levantado y muerto cada un cierto período de tiempo vía cron, y que al morir nos deja los datos que colectó en un archivo. Este archivo es interpretado por su frontend, que nos muestra los datos vía web. Es bastante potente, e intuitivo.
Su ubicación ideal sería en el mismo host que monitorea el tráfico con Snort, o sea, detrás de los firewalls principales.

- Monitores de estado de red:

Los monitores de estado de red más populares son Nagios (13) y el autóctono JFFNMS (14). Ambos ofrecen la posibilidad de monitorear el estado de los distintos nodos de la red en tiempo real, no sólo para ver si siguen vivos, sino además en cuanto a su "salud" (uso de disco rígido, memoria, procesador, etc.) y a la de los servicios que brindan. Necesitan de la configuración de una comunidad SNMP para lograr ésto, pero tienen muy buenos tutoriales a disposición de quien desee probarlos. Nagios ofrece además la posibilidad de enviarnos alertas vía SMS, interactuar con él con una interfaz WAP, o que nos avise con mensajes verbales, sean éstos pregrabados, sea mediante Festival. A este respecto, recomiendo el HOWTO de Israel Ochoa (15), muy simple y descriptivo.
Podemos instalar Nagios en algún host de la red interna, y configurarlo para que monitorice la misma, así como la DMZ.

- Analizadores de vulnerabilidades:

Hay quien dice que en éste apartado, con mencionar a Nessus (16) basta. Es hoy por hoy la solución más activa a la hora de analizar los potenciales problemas en redes de muchos hosts, porque además de realizar distintas evaluaciones, nos informa de las posibles soluciones a las mismas. La comunidad detrás de Nessus es muy activa, y renueva los plugins que permiten detectar nuevas vulnerabilidades constantemente. La ventaja principal es que integra los análisis realizados por muchas herramientas en una sola interfaz, y que al trabajar por definiciones, resulta fácil mantenerlo al día. Sin embargo, si deseamos hacer las cosas a la antigua usanza, podemos caer en un set de herramientas como el descrito en http://www.l0t3k.org/security/tools/vulnerabilityscanner/. Otras herramientas y guías para realizar pen-tests están disponibles en http://www.owasp.org/index.jsp. Pero insisto, la ventaja principal de Nessus es que nos permitirá sistematizar el análisis y la interpretación de resultados.
Al igual que con Nagios y JFFNMS, nos convendrá colocar Nessus en un host de la intranet. Para analizar los hosts de la DMZ, lo más conveniente es utilizar una distro como ASC (17).

- Sistemas de alertas:

Lamentablemente, aquí no existe la solución universal (excepto por el caso de Nagios, que ya incluye esta capacidad). Deberemos customizar algún script como los de Danielle Duca (18) para la utilidad mon (19), si es que deseamos alertas vía SMS. Las alertas vía mail son fácilmente configurables en la mayoría de las aplicaciones. Otra alternativa es configurar como dirección de correo destinataria de las alertas la que en la mayoría de las compañías de teléfonos celulares está asociada al propio número de teléfono. Lo más importante al crear o montar un sistema de alertas es decidir qué queremos que nos avise, y cuándo (no es muy agradable que nos despierte el teléfono a las tres de la mañana porque hay un posible port scanning en progreso…).

- Servidores de logs:

Dependiendo del tamaño de nuestra red, nos puede resultar mucho más simple monitorear un solo servidor de logs antes que a cada host en particular. Sysklogd, el servidor de logs por defecto en la mayoría de las distribuciones, soporta logging remoto por defecto. El único problema es que los datos se envían vía UDP, con lo cual podemos perder alguna transacción ante una cogestión o caída de la red. La opción más recomendable es Syslog-ng (20). El mismo trabaja cifrando las comunicaciones entre el cliente de logs y el servidor, mediante conexiones TCP, con lo cual, nos aseguramos de recibir todos los datos en el servidor, y además evitamos fugas de información por potenciales sniffers.
Lo siguiente a pensar al instalar un servidor de logs es cómo interpretaremos los datos que de él surjan. Leer los logs guardados a ojo no es una solución muy sana para nuestra psiquis, así que en general deberemos caer en algún analizador de logs. Logwatch (21) es la utilidad que a éste respecto incluyen la mayoría de las distribuciones, y que básicamente recorre los logs del sistema en búsqueda de irregularidades, o datos que encajen con un cierto patrón. Para analizar los logs del Squid existen varias herramientas, desde la simple Squidview (22), pasando por Webalizer (incluido en muchas distribuciones), hasta llegar a Squeezer2 (23), un script que genera reportes de uso de eficiencia, por usuario, etc. Otra opción avan-

zada, pero muy recomendable, es Modlogan (24). Modlogan también es capaz de analizar los logs de Apache, así como de varios servidores FTP. El único problema es que ya no es mantenido, si bien mucha gente lo sigue usando.
Webalizer mismo nos puede servir para analizar el tráfico de Apache, generando reportes de utilización bastante detallados. Una opción más simple es AWStats (25), que además puede analizar la salida de servidores de correo y FTP. La única macana es que no es capaz de generar alertas. Y al ser un script CGI, es necesario tratar con cuidado los permisos con los que se instala y trabaja.

- Suscripción a un servicio de alertas:

Un CERT, o Computer Emergency Response Team, es un equipo (usualmente de alguna universidad o de alguna institución gubernamental) que se dedica a colectar y analizar vulnerabilidades de sistemas operativos y aplicaciones. Usualmente publican además una lista actualizada con las amenazas más activas, y brindan un servicio de alertas vía correo electrónico o RSS que se expide diariamente. Por lo general podremos configurar el canal de información que deseamos recibir, para poder acotar la cantidad de alertas que recibimos. Los más recomendables son el de la Universidad Carnegie Mellon (26), el de RedIris (27) en España, y localmente tenemos ArCERT (28). Como consejo personal, no se pongan golosos a al hora de suscribirse a un CERT. Comiencen con un par de listas de distribución, y luego, si ven que todo va bien, asóciense a otras. El volumen de datos brindado por cada una puede ser inmanejable, y más temprano que antes los terminará aburriendo…

Del papel a la realidad

El siguiente paso consiste en evaluar qué vamos a instalar, y dónde. Lo ideal es realizar un relevamiento de la red como expliqué en notas anteriores, y luego plantearnos las ubicaciones de los distintos servicios y monitores a instalar. Una vez configurados los hosts e instalados los programas, lo más conveniente será comenzar con un análisis de vulnerabilidades vía Nessus. Con el reporte brindado por ésta aplicación ya tendremos bastante para trabajar, así que tomémonos las cosas con calma. Comencemos por solucionar los fallos encontrados en los servidores y firewalls de borde. Hay que tener mucho cuidado con las actualizaciones automáticas en el caso de los servidores. Lo ideal sería basar las distintas instalaciones en una misma distribución, y en una misma release de esa distribución. Esto nos permitiría montar además un servidor de testing, donde probar las actualizaciones antes de volcarlas en masa a los servidores de producción. Ahora bien, esto sólo será posible si estamos instalando por primera vez, o sino planteamos una renovación a fondo de la infraestructura, Pero en general, deberemos lidiar con tener más de una distribución y más de una versión de cada distro instalada.
Luego, sigamos con los hosts de la intranet (de más está decir que es necesario contar con una solución antivirus para las estaciones de trabajo, así como en los servidores de correo). De nuevo, las actualizaciones automáticas deben ser manejadas con mucho cuidado, ya que nos podrían trae más de un dolor de cabeza, al modificar la configuración de algún servicio esencial.
Una pastilla sobre la organización de la intranet: si bien nos llevará más trabajo, no confiemos la asignación de direcciones IP a un servicio dinámico, como DHCP. De esta manera evitaremos posibles intrusiones por asignación de direcciones a hosts no deseados. Si es necesario manejar un pool de direcciones dinámicamente, coloquémoslas detrás de un Proxy bien monitoreado, y con capacidades limitadas a la hora de comunicarse.
A la hora de configurar el servidor de correo -y no a manera de cortesía como mucha gente piensa- configuremos las direcciones postmaster@nuestrodomino y abuse@nuestrodominio. Nos permitirán identificar alguna práctica de abuso de correo que no hayamos advertido, originada en un posible zombie alojado en nuestra intranet, por ejemplo. Y además, le haremos la vida más fácil a los administradores de otras redes.
Luego, concentrémonos en cómo centralizar las alertas de los distintos monitores, en lo posible sobre un solo host. Y por último, en función de los análisis que obtengamos de los distintos hosts, comencemos a ajustar las configuraciones de los servidores Proxy, firewalls y NIDS para mejorar el desempeño de la red, y la utilización del ancho de banda.
Una vez que creamos que tenemos el panorama más o menos dominado (escribí creamos a propósito), deberemos consensuar con los usuarios y/o personal administrativo un esquema de intervalos de mantenimiento. Dichos intervalos de mantenimiento deberían basarse en varios ciclos superpuestos.

Looping the loop

Los ciclos de mantenimiento se estructuran en función de la importancia del equipamiento a mantener, de la exposición de los mismos al resto del mundo, y de la frecuencia con la que se liberen actualizaciones para el software instalado en ellos. Pero en lo que hace a mantenimiento preventivo, deberemos realizar una agenda independiente de la de mantenimiento necesario. Dentro de ésta agenda incluiremos las auditorias y relevamientos de vulnerabilidades de los distintos hosts en la red. Para realizarlos, es conveniente que los sistemas a analizar se encuentren en condiciones lo más similares posibles a su operación normal, pero que no tengamos interferencias por tráfico. De esta manera, podremos llevar a cabo la tarea más eficientemente. Es por ésto que lo ideal sería agendar estos relevamientos para fines de semana o feriados. Un intervalo menor deberían tener los relevamientos referentes a los hosts de la intranet, pero a éstos los podremos realizar en forma pasiva, es decir analizando la salida de los monitores de red y NIDS. Para poner las cosas en claro, digamos que una vez por semana analizamos críticamente las salidas de los NIDS y monitores de red sobre los hosts de la intranet, una vez por mes auditamos las vulnerabilidades de los servidores de la DMZ, y una vez cada dos meses realizamos un mantenimiento general de la DMZ y de los firewalls, actualizando software si es necesario.
Desde luego, ante un aviso de amenaza o vulnerabilidad de riesgo alto que recibamos desde un CERT, deberemos tomar las medidas necesarias. Para la gerencia o administración puede resultar chocante, pero a veces será prudente sacar de producción un servidor que no tiene parche para una vulnerabilidad hasta que éste sea liberado. Es necesario hacerles entender ésto, porque el compromiso de los datos contenidos en él podría traernos consecuencias mayores…

Conclusiones

A simple vista, la parte más pesada de implementar un esquema de seguridad de manera responsable reside en la palabra "implementar". Pero, seamos realistas, pese a los problemas la instalación y configuración nos resultará la parte más entretenida. Es así que lo que con el tiempo se nos hará más pesado es lo representado por la palabra "responsable". La responsabilidad y el compromiso que tengamos con los esquemas de auditoria y mantenimiento serán determinantes a la hora de tener que lidiar con un problema real. Cuanto más preparados estemos, más fácil nos será sobrellevar un ataque o un problema en nuestra red…
La nota siguiente estará dedicada a aquello que más tememos, es decir, cómo lidiar con una intrusión. Nos podrá molestar, es cierto, pero tendremos que seguir viviendo, tratar de contener daños, y devolver el o los sistemas comprometidos a producción lo antes posible. Es así que, de nuevo, cuanto más previsores seamos, mejor saldremos de estas situaciones. ■

Referencias:

1- http://sourceforge.net/projects/sentrytools/
2- http://www.snort.org
3- http://sourceforge.net/projects/tripwire
4- http://www.cs.tut.fi/~rammer/aide.html
5- http://www.chkrootkit.org/
6- http://www.ossec.net/
7- http://bro-ids.org/
8- http://www.nersc.gov/nusers/security/TheSpinning-Cube.php
9- http://www.mynetwatchman.com/
10- http://www.ntop.org
11- http://www.sp.uconn.edu/~jrifkin/ipaudit/
12- http://ipaudit.sourceforge.net/ipaudit-web/
13- http://www.nagios.org
14- http://www.jffnms.org/
15- http://nagios.linuxbaja.org/
16- http://www.nessus.org
17- http://www.remote-exploit.org/index.php/Auditor_main
18- http://www.danieleduca.it/smsmon.php
19- http://www.kernel.org/software/mon/
20- http://www.balabit.com/products/syslog_ng/
21- http://www.logwatch.org/
22- http://www.rillion.net/squidview/
23- http://www.rraz.net/squeezer2/
24- http://modlogan.org/
25- http://awstats.sourceforge.net/
26- http://www.cert.org/
27- http://www.rediris.es/cert/
28- http://www.arcert.gov.ar/





Conozca cómo las aplicaciones pueden transformar las comunicaciones de su negocio
AVAYA
MOVILIDAD
Correo Electrónico, teléfono, video, fax… usted decide. Ofrezca a su personal acceso completo y seguro desde cualquier lugar.
MENSAJERÍA
Distribuya información y herramientas de gestión personal en forma inmediata a las personas que lo necesitan y de la forma deseada.
TELEFONÍA IP
Unifique todas sus aplicaciones con telefonía IP, migre a la nueva tecnología cuando lo desee. Soluciones IP puras o mixtas para todo tipo de empresas.
CONTACT CENTER
Proporcione la resolución de problemas y contacto con el cliente con mayor y mejor capacidad de respuesta. Obtenga una visión completa de sus clientes.
SOLUCIONES INTEGRALES DE COMUNICACIONES DE VOZ, DATOS E IMÁGENES
Artel Soluciones
Hi Technology in Business
AVAYA
BUSINESS PARTNER
AUTHORIZED RESELLER
SYSTIMAX SOLUTIONS
APC
AXIS COMMUNICATIONS
NETBOTZ
FAYSER
Rivadavia 893 6º Piso (C1002AAG) - Bs. As. - Argentina - Tel.: (011) 5031-8600
Mail: info@artelsoluciones.com.ar - Web: www.artelsoluciones.com.ar



Team Services Education Resources



IMPOSIBLE NO CONOCER Foundstone

Las empresas de cierta envergadura realizan adquisiciones de otras empresas. Se dice ***"dime a quién ha adquirido y te diré quién es".***

Foundstone Inc. es una de las empresas de seguridad informática de más prestigio existentes. Mc Affee en el 2003 adquirió Foundstone que hoy forma parte de ella. Invitamos a conocer foundstone y la gran cantidad de white papers y herramientas gratuitas que ofrecen al profesional de seguridad informática. Como ejemplo podrán ver en este artículo la herramienta "Hackme Bank" y algunos de libros cuyos autores trabajan en Foundstone. Seguramente todos reconocerán "Hacking Exposed". Stuart McClure es su co-autor y co-fundador de Foundstone.

HACKME BANK™ V2.0

Hackme Bank™ está diseñado para enseñar a los desarrolladores de aplicaciones, programadores y profesionales de la seguridad como crear software seguro. Hackme Bank es una aplicación bancaria online similar a la que se encuentra en el "mundo real" y basada en web services. Ésta fue construida con un número de vulnerabilidades conocidas y comunes. Ésto les permite a los usuarios realizar exploits verdaderos contra una aplicación web y por tanto aprender temas específicos y como mejor arreglarlos. Los web services expuestos en Hackme Bank son usados por otras aplicaciones ofrecidas por Foundstone en "Free Tools" incluyendo "Hackme Book" y "Hackme Travel".

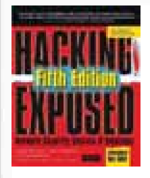
Requirimientos

Windows .NET Framework v1.1
Microsoft IIS
MSDE or Microsoft SQL Server 2000
Microsoft Internet Explorer 6.0

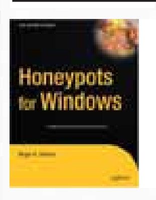
Hackme Bank™ v2.0
Copyright 2004-2006 (c)
by McAfee, Inc.
http://www.foundstone.com

LIBROS DE FOUNDSTONE

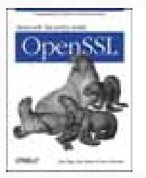
Foundstone es la fuente de conocimientos líder en seguridad de redes, y ha escrito "el libro" sobre los últimos métodos de protección.
Contando con el más calificado conjunto de talentos en seguridad jamás reunido, incluyendo a expertos de la industria de seguridad IT, los autores de Foundstone proveen los libros de referencia más ampliamente consultados en la industria de la seguridad.



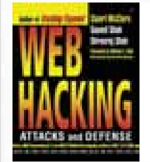
1) "Hacking Exposed: Network Security Secrets & Solutions", Osborne/McGraw-Hill. (2005) por Stuart McClure, Joel Scambray, y George Kurtz



2) "Honeypots for Windows", Apress. (2005) por Roger A. Grimes



3) "Network Security with OpenSSL: Cryptography for Secure Communications", O'Reilly. (2002) por John Viega, Matt Messier, Pravir Chandra



4) "Web Hacking: Attacks and Defense", Addison Wesley Professional. (2002) por Stuart McClure

SEGURIDAD INFORMÁTICA EN LAS EMPRESAS ARGENTINA

McAfee®

NEX IT Specialist consultó a Daniel Astudillo Vivar, Gerente de Ingeniería de Preventas Cono Sur, McAfee, Inc. sobre la situación e importancia de la seguridad informática en las empresas argentinas.

NEX: ¿Qué nivel de importancia asignan las empresas nacionales al tema de la seguridad informática?
DAV: *En la actualidad la seguridad informática juega un rol importantísimo en las empresas nacionales, ya que cada día se desarrollan e incorporan procesos del negocio que van de la mano con la tecnología informática. Sin dudas es una preocupación que la gran mayoría de los administradores de seguridad tienen en cuenta, por lo que aplican medidas de control para mitigar las amenazas presentes con diferentes políticas y herramientas. Si nos enfocamos a las grandes empresas la preocupación es mayor, y la dedicación y esfuerzos van de la mano con la inversión a proteger. Es por ésto que en las grandes empresas se hace más frecuente encontrar administradores o jefes de seguridad con dedicación exclusiva a dichas tareas, mientras que en las pequeñas y medianas, es común encontrar al administrador de red preocupado de la seguridad pero en un grado menor.*
En general la alta gerencia de las grandes empresas le ha dado el nivel de importancia que corresponde a la seguridad informática, sin embargo la administración en las pequeñas y medianas empresas están un poco retrasados, debido principalmente, a la poca información y preocupación relativa al tema informático, ya que se dedican en su gran mayoría al negoció y operación, dejando de lado los agentes externos lo que lo pueden afectar.

NEX: ¿Existe conciencia en la necesidad de invertir en este ámbito?
DAV: *Las grandes empresas le han dado importancia a la necesidad de invertir en seguridad informática, principalmente por que la gerencia ha entendido la problemática. Constantemente evalúan las soluciones que están disponibles en el mercado y eligen la que mejor relación protección v/s precio puedan adquirir. Al mismo tiempo se han dedicado a realizar auditorías de seguridad y evaluaciones de riesgo operacional no sólo a los activos informáticos, si no que abarcando el contexto global de la operación del negocio. No obstante lo anterior, creo que no se ha hecho lo suficiente respecto a lo que seguridad informática se refiere, hago hincapié también a lo importante que resulta el contar con capacitación adecuada respecto del uso de los recursos informáticos y sus vulnerabilidades más comunes, incluidas las de Ingeniería Social y el robo de identidad.*
Las empresas medianas y pequeñas se han preocupado de adquirir tecnologías de seguridad mínimas y por lo general no han realizado evaluaciones de riesgo operacional, lo anterior, principalmente por desconocimiento y la negación a aceptar que un problema de seguridad informático pudiese afectar sus sistemas. Las empresas que si lo han hecho, ha sido lamentablemente debido a alguna incidencia que afectó sus sistemas anteriormente.

NEX: ¿Qué tan necesario es que las empresas nacionales velen por temas de seguridad informática al interior de las mismas? ¿Es un tema operativo o más bien un tema estratégico?
DAV: *Toda empresa que base la operación de sus negocios sobre activos informáticos debe necesariamente velar por los temas de seguridad que los pudiesen afectar, y principalmente al interior de las mismas, ya que estadísticamente la gran mayoría de los incidentes reportados fueron cometidos dentro de las corporaciones.*
La seguridad informática es muy importante si está relacionada directamente al negocio de la empresa, y al proteger la inversión informática estamos menos expuestos a que la continuidad operacional se vea afectada. Si la empresa es afectada por incidentes de seguridad (fuga, borrado, cambios y no disponibilidad de la información) se verá afectada en su imagen y probablemente sus socios no quieran hacer negocios con una empresa que carece de seguridad; por el contrario, si demuestra preocupación por el tema, sus socios estarán mas susceptibles a tenerlos.

NEX: ¿Existe cultura empresarial acerca de la seguridad informática a nivel nacional?
DAV: *Como se ha dicho anteriormente, nos atrevemos a decir que la preocupación a nivel nacional existe pero en dos grandes grupos, grandes empresas (con encargados de seguridad con dedicación exclusiva al tema) y la PYME con conocimientos y herramientas limitadas.*

NEX: ¿Cuál es la tendencia actual en temas de seguridad informática en nuestro país?
DAV: *Sin lugar a dudas la tendencia es a una mayor preocupación, principalmente en las pequeñas y medianas empresas donde hay mucho que hacer y mejorar. A nivel nacional existen empresas de servicios y de productos con la tecnología adecuada para cada necesidad.*

Information Systems Security Assessment

Por **Hernán Marcelo Racciatti**
Senior Security Consultant
SICinformática

En ediciones anteriores, tuvimos oportunidad de presentar algunos de los aspectos que habrían hecho del OSSTMM, un estándar de facto en lo que a Testeos de la Seguridad se refiere. Llegó el turno de conocer como ISSAF, puede convertirse en nuestro aliado, al momento de poner en marcha un proyecto de Penetration Testing.



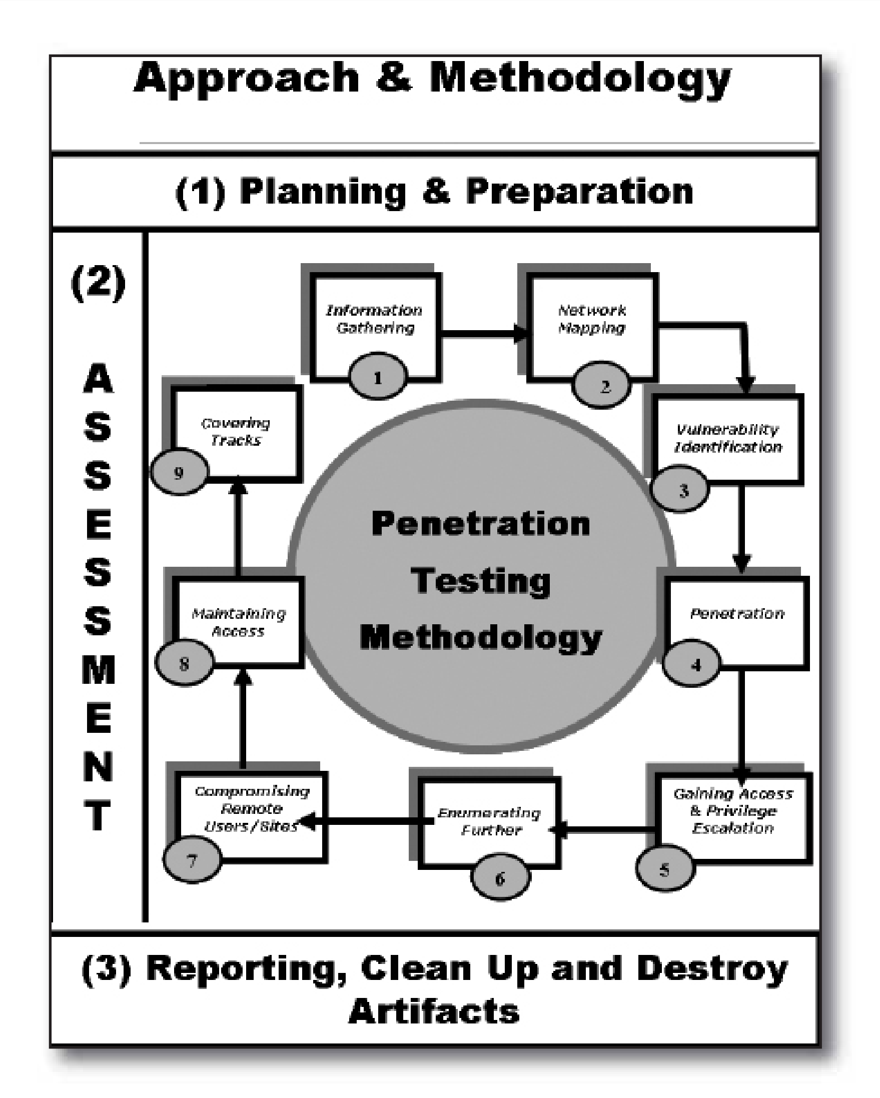
Muchas son las herramientas con las que organizaciones y profesionales, contamos a la hora de trabajar en función de minimizar el riesgo asociado a cada uno de los activos que a diario intentamos proteger. Entre éstas, las tareas relacionadas con el proceso de evaluación de la seguridad, desempeñan un rol fundamental de cara a la estrategia integral, que directamente relacionada con la "Política General de Seguridad" y por ende el negocio en sí mismo, nos permiten conocer la postura que presenta nuestra organización en general y cada uno de nuestros activos en particular.

Como probablemente sea de vuestro conocimiento, y dejando de lado el marketing que hoy en día rodea todos y cada uno de sus aspectos y términos relacionados, la seguridad sigue y seguirá siendo un proceso continuo. Como parte de dicho proceso, la evaluación de seguridad en cualquiera de sus formas (Auditing, Penetration Testing, Vulnerability Assessment, Ethical Hacking, etc.) representa a diferencia de lo que muchos consideran, tan solo un recurso más a nuestra disposición a la hora de velar por la seguridad de la información.

Hace algunos meses desde estas mismas páginas, hacíamos mención al modo en que organizaciones tales como ISECOM ("Institute for Security and Open Methodologies"), a través de proyectos como el OSSTMM ("Open Source Security Testing Methodology Manual"), habrían colaborado con la profesionalización de las tareas de testeo, convirtiendo a sus prácticas relacionadas en una actividad respetada, y proveyendo a la comunidad toda (Corporaciones, Profesionales de la Seguridad, etc.) de un documento que aproximadamente cinco años después de su aparición, se ha convertido en un estándar de facto en lo que a evaluaciones de seguridad se refiere. (Mas información sobre OSSTMM e ISECOM en NEX #20: "Testeo de la Seguridad: Una Acción Metodológica")

Quienes hayan tenido oportunidad de trabajar o al menos echar un vistazo al OSSTMM, sin dudas habrán notado que uno de sus objetivos primarios es el de definir un conjunto de reglas y lineamientos a partir de los cuales sea posible establecer principalmente CUÁNDO, QUÉ y CUÁLES eventos deben ser testeados, así como también proveer tanto al profesional a cargo del proyecto de testeo como al cliente, de un marco estándar y consistente así como resultados claramente cuantificables, mediante los cuales sea posible garantizar los resultados, la exactitud y la validez de las pruebas realizadas.

A diferencia de la metodología desarrollada en el OSSTMM, el framework que revisaremos juntos en esta oportunidad, se encuentra más enfocado a resolver el CÓMO, lo que sin dudas nos permitirá aprovechar la información en él contenida, para complementar las sentencias generales dispuestas a lo largo de las diferentes metodologías, incluyendo el prestigioso manual de ISECOM sobre el cual hemos centrado nuestra atención en números anteriores, o por supuesto utilizarlo de modo exclusivo dependiendo las circunstancias. En tal sentido, debido a la naturaleza modular de este framework, siempre tendremos oportunidad de utilizar módulos independientes, un subconjunto de ellos o el framework en forma íntegra.



Conociendo ISSAF (Information Systems Security Assessment Framework)

Tal como su nombre lo indica, ISSAF es un framework desarrollado por el grupo de tareas de OISSG a cargo de Balwant Rathore (Ver Destacado: "Acerca de OISSG"), en el cual es posible encontrar cada uno de los diferentes aspectos relacionados con la evaluación de seguridad de los sistemas de información, divididos en grandes categorías claramente diferenciadas, las cuales comúnmente referidas como dominios, incluyen información detallada respecto de tareas especificas a realizar, así como también el criterio de evaluación individual recomendado para cada una de las mismas.
Uno de sus objetivos principales, es el de proveer al profesional de seguridad de la información, de la experiencia de campo obtenida por el equipo de desarrollo de OISSG conformado por expertos en los diferentes dominios, en la realización de evaluaciones de seguridad y tareas de assessment en escenarios reales, de modo tal que la misma sirva como una guía efectiva al momento de evaluar de modo práctico cualquier tipo de sistema de información y mejorar su nivel de seguridad.
ISSAF no solo hace referencia a tareas de testing o evaluación, sino que también incluye información respecto a los diferentes procesos involucrados en una estrategia de seguridad tradicional. De este modo, es posible encontrar descripción de procesos de hardening, checklist o listas de comprobación para algunos de los productos de software o tecnologías más populares, y mucha otra información relacionada con diversos controles de seguridad.
Como mencionamos anteriormente, ISSAF se encuentra organizado de acuerdo a criterios de evaluación, cada uno de los cuales ha sido revisado por expertos en cada dominio. Para cada uno de estos, el framework incluye una estructura compuesta por los ítems mencionados a continuación, de modo de facilitar su lectura y puesta en práctica:

- Una descripción del criterio de evaluación.
- Sus objetivos.
- Los pre-requisitos para llevar a cabo la evaluación.
- El proceso de evaluación.
- Exhibición de los resultados esperados.
- Contramedidas recomendadas.
- Referencias a documentos externos.

Un aspecto interesante de ISSAF, es como hemos mencionado, que a diferencia de muchas otras metodologías o frameworks, éste habla no sólo acerca de QUÉ/CUÁNDO/DÓNDE sino también del CÓMO. Éste es el motivo por el cual a lo largo de ISSAF, no sólo encontrará sentencias de alto nivel o referencia normativa, sino que tal vez lo más rico de este framework, se encuentre en aspectos tales como: técnicas de assessment concretas, ejemplos con herramientas de uso frecuente, referencias a documentos puntuales relacionados con las tareas de testing de cada uno de los dominios, o controles concretos a implementar como parte de las contramedidas.
A pesar de ello, ISSAF no solo se concentra en lo técnico. A lo largo del framework, es posible encontrar mucha y variada información respecto de aspectos tales como: evaluación de riesgos, referencias a la administración de proyectos, formularios y documentos tipo (Templates) a utilizar en las tareas de evaluación, información respecto del armado del laboratorio de pruebas con el que el profesional debería estar familiarizado antes de realizar pruebas en las instalaciones del cliente, conceptos de BCP (Plan de Continuidad de Negocios) y DRP (Plan de Recuperación ante Desastres), pautas para la conformación de equipos de trabajo y mucha otra información sin desperdicios.

ISSAF: Penetration Testing Methodology

Sin dudas, uno de los aspectos alrededor de ISSAF que concentra mayor atención por parte del publico en general, se encuentra relacionado principalmente con la sección de nombre "Technical Controls and Security Assessment", en la cual se incluye entre otros puntos, la metodología de Penetration Testing propuesta por OISSG. Ésta, se compone de tres fases principales y nueve pasos de evaluación, y ha sido diseñada específicamente para evaluar red, sistemas y aplicaciones. A efectos de que el lector pueda obtener un primer vistazo de dicha metodología, a continuación citaremos una breve descripción de lo que incluye cada una de estas fases, así como su objetivo principal:

PHASE I: PLANNING AND PREPARATION

Esta primera fase, involucra aspectos tales como el intercambio de información inicial entre el cliente y el equipo de evaluación, el planeamiento, y la preparación del test. Entre las tareas principales, se encuentra la confección y firma de ambas partes de un documento conocido como "Assessment Agreement", el cual provee básicamente protección legal tanto al equipo al que se le ha encargado el Penetration Test como al cliente. A su vez, dicho documento especifica también, aspectos tales como el rango de fechas en las que serán llevadas a cabo las tareas, el tiempo total de duración del Test, el alcance en cuanto al escalamiento de sistemas dentro del cliente, y cualquier otro aspecto que deba ser acordado previamente.
A modo resumen, a continuación se mencionan algunas de las tareas que entre otras conforman esta primera fase:

- Identificación y Registro de la Información de contactos individuales de ambas partes.
- Reunión de confirmación de alcance y comunicación de approach y metodología a utilizar a lo largo del Test.
- Acuerdo respecto de los test específicos a realizar, así como también de los límites de escalamiento.

PHASE II: ASSESSMENT

Este es el paso en el cual se realiza el Penetration Test, utilizando para ello un approach comúnmente referido como Layered, en el cual cada capa representa un nuevo nivel de acceso en el cual su información es evaluada. A continuación, se mencionan los nueve pasos que componen la fase de Assessment, cada uno de los cuales posee su propia sección dentro del framework, a partir de la cual es posible acceder a información detallada respecto de la lista de tareas a realizar en cada paso:

1. Information Gathering
2. Network Mapping
3. Vulnerability Identification
4. Penetration
5. Gaining Access & Privilege Escalation
6. Enumerating Further
7. Compromise Remote Users/Sites
8. Maintaining Access
9. Covering Tracks

PHASE III: REPORTING, CLEAN UP & DESTROY ARTIFACTS

Como su nombre lo indica, en esta fase se completan las tareas de reporting, limpieza y destrucción de artifacts. Respecto del trabajo de reporting, ISSAF provee una serie de consideraciones y recomendaciones generales en cuanto a su forma y estructura, a la vez que se mencionan algunos puntos de existencia obligatoria entre los que se encuentran:

- Resumen Ejecutivo
- Alcance del Proyecto (y partes fuera de alcance!)
- Herramientas que han sido utilizadas (Incluyendo cualquier tipo de exploit)
- Información respecto de Fecha y Hora en la que los test fueron realizados
- Cada salida individual de cada uno de los test llevados a cabo (Excluyendo escaneos de vulnerabilidades los cuales pueden ser incluidos como attachments)
- Lista de todas las vulnerabilidades identificadas incluyendo recomendaciones de cómo cada una de ellas puede ser mitigada.
- Lista de acciones a tomar (Prioridades, soluciones recomendadas, etc.)

Respecto de las tareas de Clean-Up & Destroy Artifacts, toda información que haya sido creada y/o almacenada sobre los sistemas testeados, debe ser removida. Si por alguna razón, no fuera posible eliminar artifacts en algún sistema remoto, cada uno de estos archivos así como su localización, deben ser mencionados en el reporte técnico, de modo tal que los mismos puedan ser identificados y removidos por el staff técnico del cliente, una vez recibido dicho informe.

ISSAF: Disponible para su descarga

Al momento de escribir este artículo, la última versión del framework ISSAF publicada y disponible para su descarga en el enlace del sitio oficial de OISSG mencionado al final del presente artículo, es el Draft 0.2.1 (01-05-2006), lo cual indica que si bien es posible identificar varias secciones incompletas, las mas de mil trescientas paginas de extensión del mismo, sin dudas resultaran de utilidad a cualquier persona u organización que relacionada de uno u otro modo con la Seguridad de la Información, encontrarán en ellas un recurso invaluable a la hora de llevar a cabo proyectos relacionados con este ámbito.

Como dato adicional, cabe mencionar que en esta ultima entrega, el equipo de desarrollo de ISSAF ha decidido dividir el documento original en dos partes a fin de simplificar su lectura: "ISSAF0.2.1A" y "ISSAF0.2.1B". La primera de ellas nuclea los aspectos relacionados con el gerenciamiento de proyectos y buenas practicas de assessment, mientras que la segunda contiene los capítulos técnicos referidos puntualmente a Penetration Testing.

Conclusión

ISSAF es un proyecto nuevo, el cual aún necesita mucho trabajo por parte de la comunidad a fin de conseguir la madurez que hoy en día ostentan proyectos tales como el OSSTMM. A propósito de este punto y a pesar de encontrarse ISSAF en etapa de borrador, si bien es cierto que en muchos casos existe un solapamiento en algunas áreas

Acerca de OISSG

OISSG (Open Information Systems Security Group), es una organización internacional sin fines de lucro, cuyo objetivo principal se encuentra relacionado con la difusión de diferentes aspectos relacionados con la seguridad de la información. Actualmente, cuenta con 39 Capítulos o Chapters distribuidos en 22 países. Su visión, se encuentra centrada en establecer un entorno donde entusiastas de la seguridad de todo el mundo, compartan y construyan conocimiento. Con el fin de lograr su objetivo, OISSG trabaja junto a la comunidad profesional, a fin de determinar necesidades, desarrollar, entregar, y promover programas que agreguen valor a la comunidad respecto de temas relacionados con la Seguridad de la Información.

Proyectos en Desarrollo:

- Information Systems Security Assessment Framework (ISSAF)
- Computer Crime Investigation Framework (CCIF)
- Capture the Flag (CTF)
- Security Essentials Framework (SEF)
- FIST Briefings
- Vulnerability Research
- Password Research
- Vulnerability Disclosure Policy (VDP)
- Metacortex-NG



respecto del OSSTMM, muchos encontraran que juntos pueden ser vistos como un gran complemento el uno del otro.

Visto desde un punto de vista general, ISSAF pretende ser amplio y detallado, de este modo aspectos puntuales como la evaluación de sistemas AS400, dispositivos de red, dispositivos móviles, VPNs, etc. encuentran en este framework tratamiento pormenorizado. La idea en torno a ISSAF, es de algún modo la de incluir tanta información como sea posible, lo cual a menudo incluye aspectos tales como: ejemplos de técnicas de testeo, las salidas de algunas herramientas y otro tipo de cuestiones similares. Este approach pose ventajas y desventajas. Entre las ventajas, podemos mencionar el invalorable recurso de poseer al alcance de la mano y en un solo sitio, información concreta respecto de cómo conducir un proyecto de Security Assessment para un amplio rango de procesos y sistemas. Sin embargo, ésto implica que el esfuerzo dedicado a mantener actualizado este framework es verdaderamente MONUMENTAL y debe ser un aspecto a cuidar a fin de que el proyecto continúe vigente, de modo tal que la información en el dispensada continúe siendo efectiva en un ciento por ciento a través del tiempo.

Para concluir y a efectos de llevar estos conceptos al plano práctico, podríamos determinar que el OSSTMM al encontrarse quizás mas enfocado a nivel metodológico, se encuentra menos afectado por factores que puedan volverlo obsoleto, pudiendo usted utilizar la misma metodología cuantas veces quiera en el tiempo, haciendo uso de diferentes técnicas y herramientas. ISSAF en cambio, es un framework el cual pretende darle la última información sobre técnicas, herramientas, mejores prácticas y regulaciones, ya sea que usted utilice OSSTMM o cualquier otra metodología.

Por último, sea que usted vaya a utilizar ISSAF como parte de su trabajo o no, apuesto a que su sola lectura, sin lugar a dudas le resultará apasionante. Quizás usted no se encuentre interesado en la parte regulatoria o de administración de proyectos de assessment, pero le resulte atractivo conocer algo más acerca de las técnicas de testing; quizás no le interese el modo en el que debe ser configurado un webserver en forma segura, pero se sienta atraído respecto de las diferentes iniciativas de awareness mencionadas en el framework. De uno u otro modo, si cualquiera de las partes de este extenso trabajo, ha servido en algún punto para elevar el nivel de seguridad de sus sistemas, o colaborado a que cada vez más personas entiendan los riesgos asociados a las tecnologías de información, sin dudas el trabajo del equipo de OISSG no habrá sido en vano y una vez mas podremos mirar fascinados, lo que la ardua tarea detrás de proyectos Open Source puede generar cuando se lo propone. ■

Acerca de Hernán Marcelo Racciatti

Hernán Marcelo Racciatti es miembro del Core Team de ISECOM (Institute for Security and Open Methodologies) y Coordinador del Capitulo Argentino de OISSG (Open Information System Security Group). Actualmente se desempeña como Senior Security Consultant en SIClnformática, asesorando y capacitando a compañías del sector público y privado, conduciendo test de intrusión controlados y como orador en conferencias relacionadas con su especialidad.

Referencias y Lectura Complementaria

- OISSG: Open Information Systems Security Group
http://www.oissg.org

- ISSAF: Information Systems Security Assessment Framework
http://www.oissg.org/issaf

- ISECOM: Institute for Security and Open Methodologies
http://www.isecom.org

- OSSTMM: Open Source Security Testing Methodology Manual
http://www.isecom.org/osstmm

- Puntos de vista respecto de las diferencias entre ISSAF y OSSTMM
http://seclists.org/lists/pen-test/2006/Apr/0222.html

- Presentaciones varias respecto de OISSG e ISSAF
http://www.hernanracciatti.com.ar





#1 El negocio del Software: Caso de Éxito Snoop Consulting
#2 Gente, Procesos y Métodos (Métodos ágiles y disciplinados)
#3 Modelado y diseño de sofware (De la nada al software, hoy)
#4 Quality Assurance de Software
#5 JAVA vs. .NET
#6 Data Warehouse, Bussiness Intelligence y Data Mining
#7 Coordinando procesos de negocios con BPEL

Modelado y diseño

De la nada al software, hoy

Bruno Forchieri
Senior Solution Architect
Snoop Consulting S.R.L.

Modelar puede ser una manera eficaz de manejar la complejidad del desarrollo de software. Permite la comunicación, diseño y entendimiento de requisitos, arquitecturas, software y sistemas. A pesar de estas virtudes, el desarrollo de software todavía no saca el suficiente provecho del modelado en el día a día de hoy.

¿Por qué modelar el software?

¿Por qué modelar algo antes de construirlo? Quizás no sea realmente necesario. Las cosas simples no necesitan necesariamente ser modeladas antes de su construcción, tales como un utilitario de conversión de monedas, una cucha de perro o una simple macro en un procesador de texto que imprima cuatro copias del documento activo.

Esos proyectos tienen alguna o todas estas características:

- El dominio del problema es muy bien conocido
- La solución es relativamente fácil de construir
- Se requiere la colaboración de muy pocas personas para construir la solución
- Es poco probable que el alcance de las necesidades futuras crezca substancialmente
- La solución requiere poco o nulo mantenimiento

En estos casos, se hace difícil justificar la necesidad del modelado; pero supongamos que ninguna de estas características es válida. No es ni económica ni técnicamente acertado construir ciertas clases de sistemas complejos sin primero crear un diseño, un modelo o alguna otra repre-

FOTO: Purdue News Service photo/Dave Umberger

sentación abstracta. Mientras que un arquitecto puede construir una cucha de perro sin un diagrama de diseño, nunca intentará construir un edificio de oficinas de 25 pisos sin un arsenal de planos arquitectónicos, diagramas y un una maqueta para la visualización.
Modelar puede ser una manera eficaz de manejar la complejidad del desarrollo de software. Permite la comunicación, diseño y entendimiento de requisitos, arquitecturas, software y sistemas. A pesar de estas virtudes, el desarrollo de software todavía no saca el suficiente provecho del modelado en el día a día de hoy.

Breve historia del modelado

En sus orígenes, el software era construido de una manera secuencial o lineal, es decir, consistía en una serie de pasos sucesivos con estructuras de control y bifurcaciones. Los programas desarrollados en esta forma, de "spaghetti", no ofrecían flexibilidad ante cambios o mejoras, por lo que el mantenimiento de una gran cantidad de líneas de código en un sólo bloque se volvía una tarea bastante complicada.
Entonces, frente a esta dificultad aparecieron los lenguajes estructurados de programación (Pascal, C y Cobol, entre otros). La idea principal de esta forma de programación radicaba en diferenciar las partes del programa según su función y separarlas en módulos o subprogramas que fueran ejecutados según sean requeridos. De esta manera, al momento de tener que realizar tareas de mantenimiento en el sistema –corrección de errores o agregados de nueva funcionalidad– era más simple para el programador localizar el punto justo a modificar en todo el sistema completo. Cosa que nunca hubiera sido así, por ejemplo, en un gran programa de 1.000.000 de líneas de código. Además, se lograba reutilizar a dichos módulos empaquetándolos en librerías o unidades, dependiendo del lenguaje.
Ahora bien, ¿Cómo determinar qué funcionalidad distribuir en cada módulo para obtener una alta cohesión entre las funciones de cada uno? ¿Cómo hacerlo de manera tal que los módulos no queden dependientes todos entre sí y en lugar de tener código "spaghetti" pasemos a tener "un plato de spaghetti"? Es aquí donde nace la necesidad de trasformar al programador en un diseñador con capacidad de obtener diseños modulares en base a los requerimientos del sistema, antes de empezar a programarlos. Por aquel entonces, el diseño modular estaba marcado por las ideas de Edward Yourdon, los diagramas de flujo de datos y las cartas de estructura. Éstas últimas eran diagramas que representaban a los diferentes módulos de una transacción que se realiza dentro de un sistema, a sus archivos o almacenamientos de información, a las relaciones y a las dependencias entre los módulos y los datos que debieran viajar entre ellos. Mediante estas herramientas se diseñaba el sistema antes de empezar a programarlo. A medida que los sistemas aumentaban su tamaño y complejidad, este estilo de programación fue reemplazando al estilo "spaghetti" propuesto por la programación lineal.
Ésto se siguió dando en torno a descomponer más y más al programa, ya que la tendencia en pleno crecimiento requería crear sistemas cada vez más grandes y complejos; lo que llevó a los desarrolladores de software a pensar en una nueva forma de programar que les permita crear sistemas de niveles empresariales y con reglas de negocios muy complejas.
Para dichas necesidades ya no era suficiente la programación estructurada ni mucho menos la programación lineal. Es así como aparece la programación orientada a objetos (POO). La POO viene del perfeccionamiento de la programación estructurada; básicamente la POO facilita la programación con los nuevos conceptos que introduce y una nueva filosofía en lo referente al diseño. La POO se basa en dividir el problema a resolver en pequeñas unidades lógicas de código que representen la realidad. A estas pequeñas unidades lógicas de código se les llama objetos. Los objetos son unidades independientes que se comunican entre ellos mediante mensajes.

> **"En el 80% de los currículms vitae que analizo noto que existe un punto referido a algún nivel de conocimientos de UML."**

UML, ¿Qué es y qué no es?

Después de casi veinte años de evolución desde la programación estructurada, nos encontramos hoy con el paradigma de Programación Orientada a Objetos totalmente instaurado como la manera inteligente de producir software. Incluso actualmente se presentan otras variantes interesantes que exploraremos más adelante en esta nota.
UML, con casi diez años de vida y una tímida versión 2.0, sustenta la cualidad de ser el lenguaje estándar de modelado por excelencia e independiente del lenguaje de programación que se pretenda usar. UML no es una metodología, por lo cual no tiene asociados un conjunto de entregables a generar. Sin embargo proporciona varios tipos de diagramas que, cuando se utilizan dentro de una metodología dada, aumenta la facilidad de entender la aplicación bajo desarrollo.
UML tampoco es un producto de software ni un IDE de desarrollo. Si bien existen varias herramientas que permiten generar diagramas UML.

Modelos de análisis

Modelo de casos de uso

El modelo de casos de uso se trata de una técnica muy difundida para capturar los requerimientos funcionales y no funcionales del sistema. Cada caso de uso contiene uno o más escenarios que representan las distintas maneras en las que el usuario u otro sistema (actores) interactuarán con el sistema a desarrollar para cumplir con un determinado objetivo. Los casos de uso deben concebirse estrictamente desde la perspectiva que el usuario tiene del sistema y redactarse consecuentemente; es decir, usando el vocabulario referido al negocio del usuario y no el técnico del analista funcional. No deben incluirse en las especificaciones de los casos de uso cuestiones relacionadas con la modificación de registros de la base de datos o cuestiones similares.
Las diferencias entre el significado de un término en un lenguaje y el otro pretende ser equilibrada mediante un documento específico: el Glosario.

Modelo de dominio

El modelo de dominio es una visualización de los conceptos que manejará el sistema. El mismo intenta representar la realidad en la que se concentra el sistema. A partir de las relaciones establecidas entre los actores y el sistema, empiezan a surgir un grupo de entidades que el sistema deberá contener. Dichas entidades con sus atributos o propiedades y las relaciones entre ellas, se plasman en un modelo gráfico de dominio. Estrictamente hablando, el modelo de dominio, es un modelo de clases UML, donde las entidades se representan según el componente gráfico asociado en dicho lenguaje.

Modelos de diseño

Modelo de clases

La célula básica del diseño orientado a objetos es el modelo de clases. En el diagrama de clases se exponen las clases con sus jerarquías, asociaciones, composiciones, atributos y métodos.
Este diagrama mantiene una absoluta vigencia y es el más usado hoy en día para representar las clases que componen un sistema dado.

El Arquitecto de Software, hoy

Lejos de la imagen del "Arquitecto" de la trilogía Matrix, el Arquitecto del sistema es hoy el diseñador general e integrador de la aplicación. Es responsable por realizar el diseño del los principales componentes y por mantener la integridad conceptual de la arquitectura. Además, es el encargado de asegurar la calidad técnica de los productos de trabajo entregados por el equipo del proyecto, incluyendo diseños, especificaciones y otra documentación. En ese sentido, también programa los mecanismos y las funcionalidades para validar las arquitecturas que presenta, sería un error no hacerlo.

Evolución de los modelos en RUP

Iterativo, reducción de riesgos

En un proceso de desarrollo de software iterativo, se busca dividir a cada actividad del proyecto (análisis, diseño, desarrollo, prueba e implantación) en varias iteraciones incrementales. Y planificar cada iteración con el objetivo de reducir todos los riesgos, sobre todo los inherentes a la construcción, lo más temprano posible en la duración del

FOTO: Purdue News Service photo/Dave Umberger

proyecto. Ésto se basa en que la manifestación de un riesgo tiene un impacto cada vez mayor a medida que avanza el reloj del proyecto.
Un ejemplo de ésto sería asumir que la integración con un sistema externo al que se está desarrollando es muy fácil y no representa riesgos por lo que el desarrollo de la misma queda relegado frente al de una funcionalidad simple que es clave para el cliente. Ocurre entonces que al momento de desarrollar dicha integración, pocas semanas antes del fin del proyecto el equipo de desarrollo detecta que existe una incompatibilidad total en los protocolos de intercambio de información; y resolverlo llevará 4 meses más. Haber tomado la precaución de evaluar al detalle dicha integración al inicio del proyecto hubiera arrojado el mismo resultado, sólo que las alternativas de acción hubieran sido muchas más y el riesgo, muy posiblemente absorbido.
Ante ésto, los modelos de análisis y diseño evolucionan durante todo el proyecto. Es decir, el modelo de dominio sólo contiene las entidades relacionadas con los casos de uso especificados en la iteración en curso y en las anteriores. Pero no se especifican todos los casos de uso ni se plantea el modelo de análisis 100% completo antes de empezar con el diseño y la implementación.

Diseño para mañana

Reusable Software Assets (RSA)

Las compañías requieren muy a menudo una manera de organizar los activos existentes para transformarlos en activos reutilizables. Un "activo reutilizable de software" es, en el sentido más amplio, cualquier colección cohesiva de artefactos que solucionan un problema o un grupo específico de problemas, en un contexto dado. Pueden tener alguna variación para contemplar requisitos particulares del consumidor del activo, y reglas para el uso que son las instrucciones que describen cómo el activo debe ser utilizado. Los artefactos son cualquier producto que se genera en el ciclo de vida del desarrollo del software, por ejemplo documentos de requisitos, modelos, archivos de código fuente, descriptores de despliegue, test cases o scripts, etc.
La especificación de activos reutilizables define una manera estándar de empaquetar dichos activos del software, el objetivo es establecer un sistema de pautas prácticas y específicas sobre cómo describir activos reutilizables para:
1. Facilitar y mejorar la comunicación entre los productores y los consumidores del activo.
2. Representar los activos en herramientas de desarrollo del software
3. Proporcionar los medios para la gestión e intercambio del activo
El OMG (Object Management Group) ha aprobado un RFC propuesto por varias empresas de software denominado "Reusable Software Asset Specification" (RAS) que logra ésto definiendo un sistema de términos relacionados con el desarrollo basado en activos y definiendo la mínima información estructurada que es requerida para facilitar la reutilización de dichos activos.
RAS describe a los activos como parte del Asset Based Development (ABD) que complementa la arquitectura dirigida por el modelo (MDA), describiendo la producción, el consumo, y la gestión del activo. Cada activo reutilizable debe contener como mínimo un archivo "manifest", y por lo menos un artefacto que se considerará un activo reutilizable válido. Un archivo "manifest" es un documento XML que valida contra uno de los esquemas XML conocidos de RAS. Un paquete de activos es la colección de archivos de artefactos más un archivo "manifest".



Enterprise patterns

Hoy en día las empresas de alto rendimiento en el desarrollo de software tienen y se nutren de un repositorio propio de patrones propios identificados mediante RSA, ésto les permite ganar productividad reaprovechando el conocimiento circulante en la empresa.
Una vez que existe una solución que es probada para un problema y un contexto dados, todos los artefactos de dicha solución deben ser catalogados mediante RSA y archivados en un repositorio común de acceso para todo el equipo de desarrollo. En algunos casos ésto se puede implementar en un file system compartido, pero lo más correcto sería un sistema de administración de versiones (CVS, SubVersion, Microsoft Visual SourceSafe, etc.); dado que dicho activo reutilizable puede verse modificado por cambios y mejoras.
Por otro lado, muchas herramientas de modelado y diseño de software soportan la conexión a un repositorio de este tipo para brindarles a los arquitectos y desarrolladores acceso a los patrones corporativos para realizar sus tareas.

Buenas y malas prácticas

Experiencia – se nace y se hace

Siempre, no importa cuánto tiempo se haya invertido en diseñar cada detalle, al finalizar la construcción de una determinada porción del sistema surge (casi como una visión divina) la pregunta: ¿Ésto o aquello no podría haberse hecho mejor de otra manera?

Los problemas ante ésto son dos. Por un lado, la porción del tiempo total del proyecto necesaria para haberlo hecho de esa manera ya fue invertida y, por otro lado, el costo en horas de desarrollo ya fue también incurrido. Con lo cual, sólo pensar en volver a construir esa parte con un nuevo diseño es casi imposible. Pero ésto tiene una ventaja, la experiencia; que, hubiera elegido la solución correcta antes de empezar y, se acaba de nutrir por no haber acertado.

Ante ésto, es importante resaltar que no cualquier programador, diseñador, o arquitecto por más conocimientos que tenga va a dar con la mejor solución a un determinado problema. Es la experiencia –sumada a los conocimientos- lo que resulta en una aproximación mayor al diseño óptimo.

Ingeniería inversa – un mal necesario

La ingeniería inversa es lograr que el diseño cumpla con el código generado; al revés de lo que realmente debiera ser. Si bien tiene sus contraindicaciones, resulta una herramienta sumamente útil al momento de enfrentarse a un software desconocido que debe ser modificado, extendido o, lo que es peor, corregido. Ya que rápidamente es posible obtener un diagrama de todas las clases existentes con sus jerarquías y relaciones que permite gozar de una visión global para empezar el trabajo.

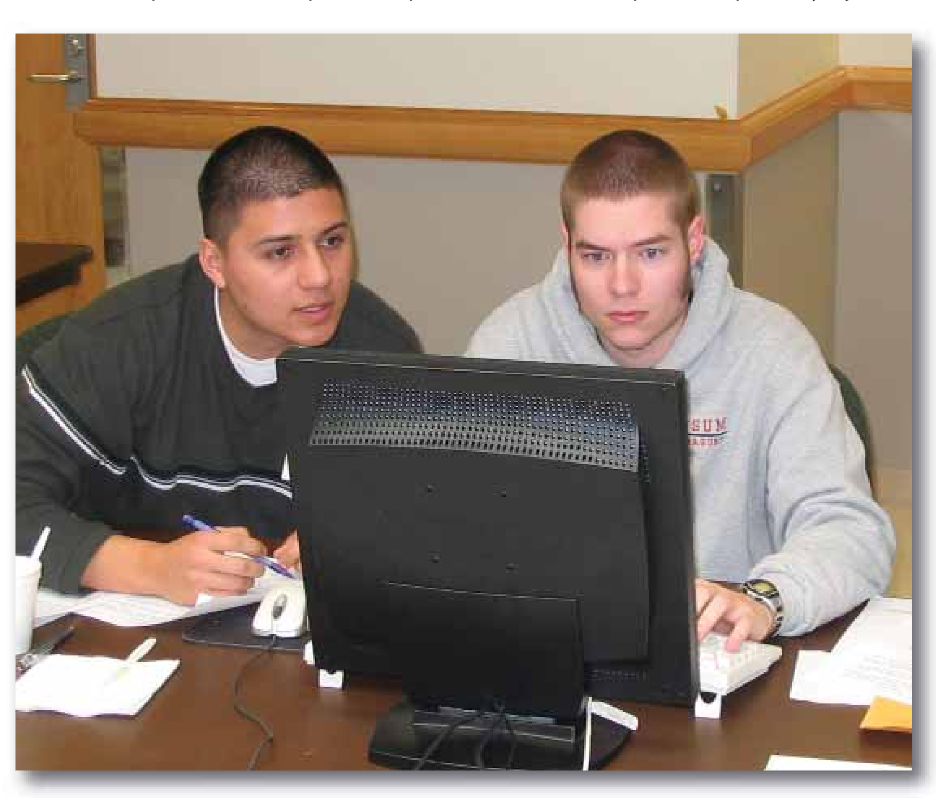


FOTO: Purdue News Service photo/Dave Umberger

Nuevas tecnologías
Nuevas arquitecturas

En los últimos tiempos el mundo del software Open Source ha liberado frameworks que han cambiado la forma de hacer aplicaciones para la Web. Un ejemplo de ésto es JSF (Java Server Faces) donde virtualmente se quiebra el paradigma request-response que durante años había dominado el terreno de este tipo de aplicaciones. JSF, en sus diferentes implementaciones (MyFaces, JSF-Spring, Project Rave, etc.) propone un modelo de listners que traduce cada interacción en la interfase de usuario en una invocación de un método de esos listeners que se configuran por cada página. Dicha invocación se no se realiza con los clásicos HTTPRequest y HTTPResponse; sino, con argumentos concretos relacionados con la información de los campos de la interfase

Por otro lado, el pattern "Dependency Injection" ha logrado disminuir en gran medida el acoplamiento entre clases con la implementación del mismo en el framework Spring.

Dependency Injection (DI) es un design pattern y un modelo arquitectónico, a veces también nombrado como Inversion of Control (IoC), aunque estrictamente hablando, la Dependency injection se refiere específicamente a la implementación de una forma particular de IoC. El pattern busca establecer un nivel de abstracción a través de una interfase pública y eliminar las dependencias entre los componentes; por ejemplo, mediante un mecanismo de plug-ins. La arquitectura subyacente será la encargada de unir los componentes, en lugar de ser los componentes los que se vinculan entre sí.

En este pattern la responsabilidad de la creación de instancias y la relación entre objetos está removida de los propios objetos y es transferida a una forma de Factory. Con un mecanismo mediante el cual se logra un muy bajo acoplamiento, lo que indirectamente resulta en objetos que pueden ser fácilmente testeados inyectándoles mock-objects. Es decir, evitando dependencias en las clases de colaboración por medio de dependencias sólo contra las interfases que son implementadas por ellas es posible producir pruebas unitarias específicas.

Las implementaciones de Dependency Injection son también conocidas como contenedores livianos (lightweight containers) por su responsabilidad en la creación de instancias de las clases definidas. Existen tres formar típicas de DI: basada en "setters", constructores y en interfases.

El framework Spring es la más conocida de las implementaciones de este pattern. Básicamente se deben definir en un XML los "beans" de la aplicación que serán inyectados a otros.

```
<beans>
        <bean id="EjemploA" class="com.snoopcon-
sulting.sample.EjemploA">
              <property name="propiedad">
                    <ref local="EjemploB"/>
              </property>
        </bean>
        <bean id="EjemploB" class="com.snoopcon-
sulting.sample.EjemploB">
              <property name="archivo">
                    <value>ejemplo.txt</value>
              </property>
        </bean>
    </beans>
```

Aquí vemos un ejemplo de un archivo de configuración donde la clase EjemploB recibe un valor String con el nombre de un archivo y la clase EjemploA requiere una instancia de una de las interfases que implementa EjemploB.

Ésto permite una absoluta flexibilidad ya que si quisiéramos ejecutar una batería de casos de prueba unitarios sobre la clase EjemploA sin que interactúe contra una instancia real de la clase EjemploB, podríamos hacerlo con solo modificar este XML.

Conclusión

Existe mal software con mal diseño, mal software con un buen diseño, pero es imposible encontrar buen software sin un buen diseño.

Bibliografía

- **Design Patterns:** Elements of Reusable Object-Oriented Software. Erich Gamma, Richard Helm, Ralph Johnson and John Vlissides. Addison-Wesley, 1995.
- **JavaServer Faces in Action,** Kito Mann, Hibernate in Action, Christian Bauer,

Lecturas Adicionales

Object Management Group (OMG)
http://www.omg.org/
Reusable Software Asset Specification 2.1
http://www.omg.org/cgi-bin/apps/doc?ptc/05-04-02.pdf
Spring (http://www.springframework.org)
Inversion of Control Containers and the Dependency Injection pattern. Martin Fowler, 2004, www.martinfowler.com/articles/injection.html



Service Oriented Architecture

¿Qué es SOA?

La Arquitectura Orientada a Servicios –por sus siglas en inglés SOA— es el enfoque de los negocios competitivos del futuro: una plataforma que permitirá a las empresas contar con una infraestructura tecnológica integrable, flexible, adaptable y de alto nivel de servicio.

Según un informe reciente de la firma de analistas Gartner, "El management SOA no es una opción, es un imperativo." De hecho, Gartner estima que la no implementación de mecanismos de gerenciamiento SOA que funcionen será la falla más común de los proyectos SOA en 2006.

¿Por qué SOA?

La base para toda Orientación a Servicios y Arquitectura Orientada a Servicios comienza con procesos de negocio. Un servicio es simplemente una tarea de negocios. Para ganar flexibilidad informática y resolver verdaderos problemas de negocio con éxito (por ejemplo, elevar la atención al cliente, integrarse con asociados de negocio o tener una visión unificada de los clientes), es crucial tener un fuerte y estrecho vínculo entre los negocios y la tecnología informática. Hoy las empresas pueden ganar flexibilidad y al mismo tiempo alinear los negocios con la IT manejando procesos de negocio a través de una SOA.

SOA usa conexiones flexibles con interfaces bien definidas y basadas en estándares para ayudar a las empresas a incorporar flexibilidad a su infraestructura existente. Los servicios SOA pueden reutilizarse extensivamente, ya se trate de nuevos servicios o activos de IT existentes.

"Brinda una infraestructura flexible y robusta para modelar, ensamblar, implementar y administrar los procesos de negocio para el ambiente de negocios on demand de la actualidad. Es eficaz en función de costos, modular y escalable, lo cual permite soluciones SOA extremo a extremo personalizadas a sus requisitos, cronogramas y prioridades" explica Silvia López Grandío, Gerente de Software de IBM Argentina.

IBM entiende la orientación a servicios y del negocio. Cuenta con las habilidades, el software y la experiencia que se necesitan para lograr flexibilidad de negocios utilizando arquitecturas orientadas a los servicios.

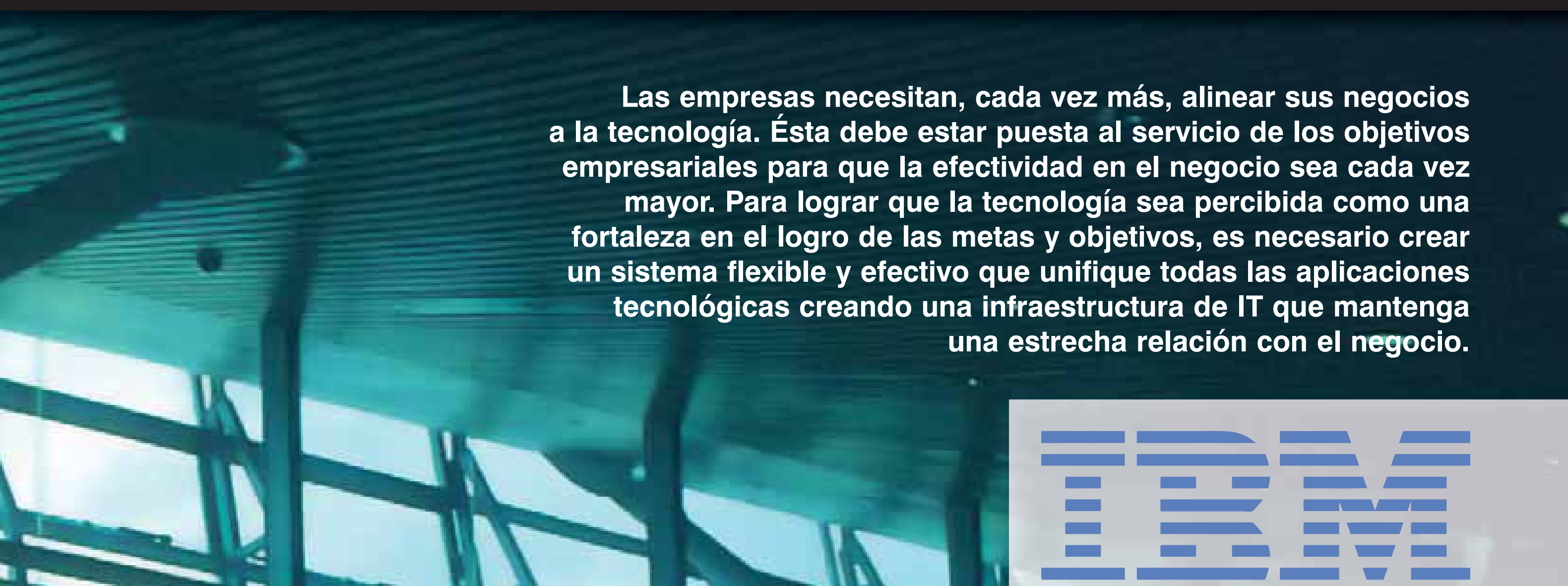
"IBM cuenta con una variedad y profundidad inigualable de productos de software para SOA. Tenemos más de 200 patentes relacionadas con SOA, hemos sido nombrados por los principales analistas del mercado como 'líderes' en ocho categorías relacionadas con SOA y hemos invertido más de mil millones de dólares por año en SOA", comenta la ejecutiva.

La extensa experiencia en la industria y mejores prácticas de IBM incluyen más de mil proyectos SOA en clientes de todo el mundo.

"Mientras que otros podrán hablar de sus estrategias SOA, IBM cuenta con la experiencia y la especialización necesarias para hacer de SOA una realidad hoy: contamos con un ecosistema próspero de asociados, tenemos aproximadamente cien mil consultores, arquitectos y especialistas en tecnología informática dedicados a SOA en todo el mundo, soluciones de negocios habilitadas para SOA y una cartera exclusiva de propiedad intelectual y métodos" destaca Lopez Grandío.

SOA: La arquitectura del cambio en IT

Hoy en día, más del 70% de las grandes empresas a nivel global implementaron SOA (Arquitectura Orientada a los Servicios) como método de centralización de los servicios en pos de un negocio



Las empresas necesitan, cada vez más, alinear sus negocios a la tecnología. Ésta debe estar puesta al servicio de los objetivos empresariales para que la efectividad en el negocio sea cada vez mayor. Para lograr que la tecnología sea percibida como una fortaleza en el logro de las metas y objetivos, es necesario crear un sistema flexible y efectivo que unifique todas las aplicaciones tecnológicas creando una infraestructura de IT que mantenga una estrecha relación con el negocio.

más rentable con un retorno sobre la inversión concreto, según información brindada por la consultora Forrester Research.

SOA es un sistema que está en pleno crecimiento y que está cambiando la manera en que las empresas compran, instalan y utilizan la tecnología. Una de las ventajas principales que presenta es que las organizaciones no perciben a la Arquitectura Orientada a los Servicios como un método duro al cuál deben adaptarse, sino todo lo contrario: es el sistema el que se adapta a la empresa según sus requerimientos, necesidades, tiempos y prioridades.

Otra de las características de SOA es que puede ser utilizada sobre activos nuevos, o reteniendo y reutilizando los activos preexistentes, ayudando a las empresas a incrementar la flexibilidad de sus procesos de negocios y fortalecer sus infraestructuras de IT. Los beneficios se hacen visibles en la resolución de los problemas reales de negocios, como la mejora en el servicio a los clientes, una mayor integración con los socios y una visión unificada de los clientes, entre otros.

Partiendo de la base de que la infraestructura de IT de una empresa debe estar fuertemente relacionada con los objetivos de negocios y una mayor eficacia en los resultados, las estrategias SOA son una efectiva y garantizada alternativa que podría ser señalada como "la nueva revolución del software".

Así mismo, la arquitectura SOA promueve la flexibilidad de la empresa; el management SOA impulsa los resultados del negocio. Las empresas están adoptando rápidamente las estrategias basadas en SOA para hacer sus empresas más modulares y mejorar el rendimiento general entre los silos de la organización, y al mismo tiempo apalancar las plataformas de tecnología. Sin embargo, SOA plantea desafíos únicos: una iniciativa SOA puede descarrilarse si no se cuenta con un marco de management eficaz para identificar claramente los roles, las responsabilidades y los derechos de decisiones relacionados con los servicios. Además, este marco debe incluir mecanismos de medición y control para asegurar mejor el cumplimiento de las políticas y brindar valor de negocios.

"La adopción de SOA es un catalizador para que una organización comience a pensar acerca de una mejor conducción corporativa y tecnológica. Al extender el management tecnológico para incluir SOA, las empresas podrán realizar plenamente el potencial de un enfoque basado en los servicios. El gerenciamiento SOA eficaz involucra más que la mera tecnología: requiere un enfoque integral de la gente, los procesos, la información y los activos de una organización", explica la responsable de software de IBM Argentina.

Oportunidad de mercado SOA

- SOA es una importante oportunidad de crecimiento para IBM y cambiará la forma en que los clientes compran, instalan y utilizan la tecnología.
- Los analistas Forrester sostienen que más del 70% de las grandes empresas ya están utilizando la arquitectura SOA.
- IDC predice que el mercado para SOA, que incluye software, servicios y hardware, llegará a los U$S 21 mil millones en 2007.
- Gartner pronostica que hacia 2008 más del 60% de las empresas usarán SOA como "principio guía" para las infraestructuras de tecnología informática.

El ciclo de vida de un Marco de Management SOA

Existen determinadas acciones que son necesarias para establecer, mantener y mejorar el management SOA eficaz. Estas acciones se describen en términos de un ciclo de vida que consta de cuatro fases: planificación, definición, habilitación y medición.

Planificación

Durante la fase de planificación de la construcción del marco de management SOA, los líderes de proyecto SOA deben enfocarse en comprender el alcance general de la necesidad de conducción dentro de la organización, e identificar áreas para mejorar.

La mayoría de estas actividades están centradas en las personas, y se enfocan en la colaboración amplia entre las gerencias de IT y de negocios. Esta fase debe concebirse como el paso dentro del ciclo de vida cuando el equipo define "el problema a tratar".

Esta fase también incluye: comprometerse con una iniciativa SOA dentro de la estrategia general de tecnología informática; determinar explícitamente el nivel de capacidades de IT y SOA; articular y refinar la visión para SOA; revisar las posibilidades y los acuerdos de management actuales, y desarrollar un plan de management general.

Liderazgo de IBM en SOA

• IBM se posicionó como líder en el Cuadrante Mágico de Gartner para Plataformas de Servicios Web (julio de 2005).
• IBM Global Services fue nombrada Market Maker Líder para SOA por IDC (agosto de 2005).
• IBM fue reconocida como la líder en SOA por AMR (septiembre 2005).
• En menos de un año, la comunidad de asociados SOA de IBM aumentó a 1000 miembros.
• IBM está invirtiendo más de mil millones de dólares en SOA este año.

Definición

Una vez identificadas las oportunidades para una mejor gestión, los profesionales de negocios y de tecnología trabajan en conjunto para definir y modificar los acuerdos y mecanismos de management actuales. Por ejemplo, éste es el momento para acordar nuevos enfoques a la creación de políticas.
Otras decisiones de conducción importantes que se toman durante esta fase incluyen: establecer o refinar un Centro de Excelencia (Center of Excellence / COE) para SOA; definir requisitos adicionales tales como actualizaciones a la infraestructura de TI; acordar políticas para la reutilización del servicio entre las líneas de negocio; implantar mecanismos de financiación para promover la reutilización, y establecer mecanismos para garantizar los niveles de servicio.

Habilitación

Durante esta fase se llevan a la acción las soluciones según la necesidad de administración. Se instalan nuevos y mejorados componentes de tecnología y procesos de management para descubrir y administrar los activos. La comunicación relativa a los comportamientos y las prácticas que se esperan dentro de las comunidades de toma de decisiones tanto de negocios como de tecnología informática resulta esencial durante esta fase para poder habilitar la infraestructura de políticas.

Medición

Finalmente, todos los acuerdos de management delineados precedentemente deben ser monitoreados, administrados y medidos. Ésto ofrece la oportunidad de evaluar los resultados y, de ser necesario, comenzar un nuevo ciclo de estas cuatro fases a fin de refinar y mejorar la eficacia del gerenciamiento.
Más aún, el análisis de la eficacia de tecnología informática y el monitoreo el cumplimiento de políticas y acuerdos de management –por ejemplo, acuerdos de nivel de servicio (Service Level Agreements / SLA), niveles de reutilización y políticas de cambio– deben ser evaluados en este momento.
"El management SOA ayuda a los clientes a establecer en la organización derechos de decisión a medida y a implementar los mecanismos de definición de políticas, mediciones y controles necesarios para poner en práctica dichas decisiones. El management eficaz ayuda a liberar a los equipos de las incertidumbres y los desafíos de tratar de definir quién necesita dar su aprobación a qué cosas, de modo que puedan concentrarse en crear y brindar soluciones de negocios innovadoras" concluye Silvia López Grandío de IBM.

10 consejos para un SOA exitoso

Si bien cada empresa tiene distintas necesidades de negocio y cada industria enfrenta su propia serie de desafíos, hay problemas comunes que pueden llevar al fracaso de una SOA. Aquí diez consejos para evitarlos:

1. Evite la falta de auspicio ejecutivo: Antes de presentar cómo asegurará el éxito del SOA propuesto en su empresa, esté preparado para demostrar éxitos y fracasos de otras compañías en su camino hacia SOA y para articular cómo emulará las prácticas comprobadas y cómo evitará las complicaciones.

2. Alinee las tropas: Contrario a superar el obstáculo del apoyo ejecutivo para su SOA se encuentra el desafío de alinear su organización para trabajar y pensar de nuevas maneras. Para hacer ésto, identifique y reclute a defensores críticos en cada parte del negocio que darán su apoyo e incluso predicarán los esfuerzos SOA.

3. Consolide visiones: Elimine las múltiples visiones de la información que actualmente flotan por la organización de modo de buscar siempre una visión singular, integral y coherente del negocio.

4. Reutilización equivale a reutilidad: Identifique y mantenga un repositorio de sus actuales servicios web para evitar la duplicación de esfuerzos. Puede sorprenderle todo el trabajo que ya se ha hecho en distintos sectores de su organización.

5. Integre los silos: Aunque en teoría muchas de las organizaciones de IT de hoy están buscando integrar y evitar redundancias y al mismo tiempo maximizar sus inversiones tecnológicas actuales, la realidad es que se están dedicando esfuerzos extraordinarios a seguir manteniendo distintos sistemas de IT que coexisten pero no están integrados. El enfoque que cuida los centavos pero no los dólares simplemente no funciona cuando se trata de un SOA.

6. Que los árboles no le impidan ver el bosque: Recuerde que un SOA es una arquitectura, no una combinación de productos puntuales juntados desordenadamente que deben encajar a la fuerza. Un verdadero SOA se crea con un enfoque basado en estándares abiertos a través de cuatro etapas estratégicas: modelar, ensamblar, implementar y administrar.

7. Súbase al Bus del Servicio Empresarial: Un ESB proporciona la infraestructura de conectividad tan necesaria que puede usarse para integrar servicios dentro de un SOA. Juntos, SOA y ESB ayudan a reducir la cantidad y complejidad de las interfaces, permitiéndole concentrarse en los temas centrales de su negocio, en lugar de en el mantenimiento de su infraestructura tecnológica.

8. Paso a paso: Cuando el pensamiento de instalar un SOA en toda la empresa se vuelve abrumador, recuerde que el mejor enfoque es probar y modificar continuamente mientras se lo implementa primero por departamentos, y luego en toda la organización, a fin de identificar problemas en tanto se va incrementando su arsenal de mejores prácticas.

9. Evite el enfoque "carpe diem": Recuerde que no está construyendo su SOA sólo para hoy o para este año. Se trata de un enfoque en toda la organización para alinear la IT con las necesidades del negocio, y debe satisfacer las necesidades de hoy y las del futuro. Por ejemplo, asegúrese de incluir soporte para dispositivos móviles e inalámbricos, así como de tener suficiente flexibilidad para estar preparado para el "próximo gran cambio".

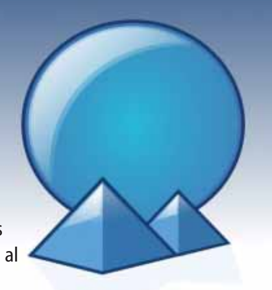
10. Evite el SOA accidental: Muchas organizaciones pueden descubrir que tienen un repositorio saludable de servicios web que integrará la mayoría de su SOA. Si bien usted no cree que el SOA comienza y termina con una colección de servicios web, recuerde que un SOA debe ir más allá de los servicios web para dar soporte a todos sus procesos de negocio. También debe brindar un enfoque flexible, extensible y componible para reutilizar y extender las aplicaciones y los servicios existentes, así como para construir nuevos. ■

Productos de IBM para SOA

IBM ha identificado cinco puntos de entrada para permitir a los clientes abordar e iniciar más fácilmente un proyecto SOA. Estos puntos de entrada incluyen enfoques centrados en las personas, los procesos y la información, así como conectividad y la capacidad de reutilizar activos existentes.

BREVES

MEPIS se muda a UBUNTU



La próxima versión de SimplyMEPIS, el SimpleMEPIS 6.0, estará basada en Ubuntu Dapper. El cambio hacia Ubuntu fue hecho para darle a los usuarios un sistema subyacente más estable. La empresa dice no haberse apartado de Debian; periódicamente Ubuntu captura el estado de Debian inestable, hace sus mejoras y correcciones de errores, y luego aporta dichas modificaciones al código fuente de Debian.
Previamente, MEPIS era miembro de la DCC Alliance (un grupo de vendores con distros basadas en Linux quienes trabajaban en un sistema base Debian en común).
El cambio ha suscitado cierta ambigüedad acerca del futuro de esta alianza ya que "no está claro hacia dónde está yendo la DCC", según Warren Woodford, fundador de MEPIS.
http://www.mepis.org



IronPort Systems es el principal proveedor de seguridad para correo electrónico corporativo, desde pequeñas empresas hasta empresas de Global 2000. IronPort ha desarrollado una familia de dispositivos de seguridad para correo electrónico, denominada IronPort C-Series™, que ofrece un rendimiento de avanzada, facilidad de uso sin precedentes y menor costo total de propiedad. IronPort está impulsando nuevos estándares y ofreciendo productos innovadores para quienes deben enfrentarse a la monumental tarea de administrar, proteger y desarrollar sistemas de correo electrónico de gran importancia.
Hoy por hoy, IronPort protege a más de 1 millón de buzones de correo electrónico en México y 4 millones de buzones en el resto de Latinoamérica.
IronPort es un startup respaldado por importantes firmas de capital.

Ya está disponible el Fedora Core 5



Esta versión de Fedora está repleta de características nuevas y aplicaciones. Kernel Linux 2.6.16, compilador GCC 4.1 e incluye Web Server Apache 2.2. Entre otras muchas nuevas características se destacan:
- Integración mejorada con el sistema de virtualización XEN.
- Inclusión del recientemente actualizado Gnome 2.14 y desktop KDE (3.5)
- El nuevo X11 R7.0 de Xorg para incrementar la performance de aplicaciones en X Window. ***http://fedora.redhat.com***

Libro recomendado:
Fedora 5 and Red Hat Enterprise Linux 4 Biblia
Autor: Christopher Negus.

SAMBA 4 Preview

El proyecto Samba ha lanzado el Samba 4.0.0TP2 (el TP significa Technology Preview).
Samba es una aplicación open source que permite compartir impresoras y archivos en sistemas Unix, Linux, y Windows, usando el protocolo de Microsoft SMB (Server Message Block) y el CIFS (Common Internet File System).
Entre sus características nuevas, la más importante es el soporte de los protocolos de logon de Active Directory (LDAP) usados por Windows 2000 y posteriores, además de integración de la herramienta de administración basada en la web (SWAT, por sus siglas en inglés, Samba Web Administration Tool), una nueva interfaz de scripting que permite a programas en javascript poder entenderse con los "Samba internals" y nuevas características de su sistema de archivos virtuales (VFS, Virtual File System). Samba 4 se encuentra aún en desarrollo y no se encuentra disponible para entornos de producción.
http://us1.samba.org/samba/ftp/samba4
http://us1.samba.org/samba/history/samba-4.0.0tp2.html

Nuevo GENTOO

El Gentoo Release Engineering team lanzó el Gentoo 2006.0. Éste usa el kernel 2.6.15, e incluye el GCC 3.4.4, y el entorno gráfico XFCE 4.2.2 lightweight.
La característica clave del Gentoo es el Portage. Esta herramienta ayuda a seguirles la pista a los paquetes de aplicaciones instalados en el sistema, y a instalar las actualizaciones de éstas. Actualmente, Gentoo soporta más de 10000 paquetes. Soporta las arquitecturas, x86, Sparc, Alpha, AMD 64, PowerPC, PowerPC64, y HP PA-RISC.
http://www.gentoo.org



Barracuda Networks, Inc. es una compañía que provee productos de firewalls para bloquear spam, virus, spyware y software de mensajería instantánea. Barracuda Networks comenzó sus actividades en 2002 y actualmente tiene sus oficinas principales en Mountain View, California (tras haberse establecido primero en Cupertino, California, durante sus primeros tres años).
El primer producto de la compañía es el appliance anti-spam llamado ***Barracuda Spam Firewall*** que corre sobre Linux. Fue lanzado al mercado en Octubre de 2003, y ha ganado desde entonces muchos premios otorgados por publicaciones. El producto acepta el tráfico SMTP y analiza la fuente y contenido de cada mensaje de correo electrónico entrante y luego toma la decisión de admitirlo, etiquetarlo, ponerlo en cuarentena, o bloquearlo. El tráfico permitido y etiquetado, es pasado al próximo sistema SMTP en la ruta, generalmente un MTA (Mail Transfer Agent) de la organización. Varios modelos pueden soportar diferentes niveles de tráfico y números de dominios. Estos sistemas pueden escalarse para permitir incrementar su capacidad y tolerancia a fallos.
En Abril de 2005 el ***Barracuda Spyware Firewall*** fue lanzado al mercado, y en Febrero de 2006 el ***Barracuda IM Firewall***.



Humor - *Por Severi*

